

AXIS A1001 Network Door Controller & AXIS Entry Manager

User Manual

About this Document

This manual is intended for administrators and users of AXIS A1001 Network Door Controller and is applicable to AXIS Entry Manager and firmware 1.25 and later. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis website, as required. See also the product's online help, available via the web-based interface.

In this manual, AXIS A1001 Network Door Controller is referred to as: the Axis product, product, network door controller, and door controller.

Liability

Every care has been taken in the preparation of this document. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at www.axis.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see www.opensource.apple.com/apsl). The source code is available from <https://developer.apple.com/bonjour/>

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.


Trademark Acknowledgments

AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC and VAPIX are registered trademarks or trademark applications of Axis AB in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.

Network Time Protocol Version 4 Distribution is copyright of University of Delaware – © University of Delaware 1992–2011. The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file. Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Regulatory Information

Europe

 This product complies with the applicable CE marking directives and harmonized standards:

- Electromagnetic Compatibility (EMC) Directive 2004/108/EC. See *Electromagnetic Compatibility (EMC) on page 2*.
- Low Voltage (LVD) Directive 2006/95/EC. See *Safety on page 2*.

- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU. See *Disposal and Recycling on page 3*.

A copy of the original declaration of conformity may be obtained from Axis Communications AB. See *Contact Information on page 3*.

Electromagnetic Compatibility (EMC)

This equipment has been designed and tested to fulfill applicable standards for:

- Radio frequency emission when installed according to the instructions and used in its intended environment.
- Immunity to electrical and electromagnetic phenomena when installed according to the instructions and used in its intended environment.

USA

This equipment has been tested using a shielded network cable (STP) and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and receiver.
 - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
 - Consult the dealer or an experienced radio/TV technician for help.
- The product shall be connected using a shielded network cable (STP) that is properly grounded.

Canada

This digital apparatus complies with CAN ICES-3 (Class B). The product shall be connected using a shielded network cable (STP) that is properly grounded. Cet appareil numérique est conforme à la norme CAN NMB-3 (classe B). Le produit doit être connecté à l'aide d'un câble réseau blindé (STP) qui est correctement mis à la terre.

Europe

This digital equipment fulfills the requirements for RF emission according to the Class B limit of EN 55022. The product shall be connected using a shielded network cable (STP) that is properly grounded.

This product fulfills the requirements for immunity according to EN 61000-6-1 residential, commercial and light-industrial environments.

This product fulfills the requirements for immunity according to EN 61000-6-2 industrial environments.

This product fulfills the requirements for immunity according to EN 55024 office and commercial environments

This product fulfills the requirements for immunity according to EN 50130-4 residential, commercial, light-industrial and industrial environments.

Australia/New Zealand

This digital equipment fulfills the requirements for RF emission according to the Class B limit of AS/NZS CISPR 22. The product shall be connected using a shielded network cable (STP) that is properly grounded.

Japan

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。本製品は、シールドネットワークケーブル(STP)を使用して接続してください。また適切に接地してください。

Safety

This product complies with IEC/EN/UL 60950-1, Safety of Information Technology Equipment. If its connecting cables are routed outdoors,

the product shall be grounded either through a shielded network cable (STP) or other appropriate method.

The power supply used with this product shall fulfill the requirements for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS) according to IEC/EN/UL 60950-1.

Disposal and Recycling

When this product has reached the end of its useful life, dispose of it according to local laws and regulations. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. In accordance with local legislation, penalties may be applicable for incorrect disposal of this waste.

Europe



This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should contact the product supplier for information about how to dispose of this product correctly.

This product complies with the requirements of Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS).

China

This product complies with the requirements of the legislative act Administration on the Control of Pollution Caused by Electronic Information Products (ACEPIP).

Contact Information

Axis Communications AB
Emdalavägen 14
223 69 Lund
Sweden

Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

www.axis.com

Supported Readers

This list of supported readers is subject to change without notice. Contact your Axis reseller for information about supported readers.

This product is compatible with UL Listed Wiegand access control readers

This product is compatible with the following RS485 access control readers:

AXIS A4011-E Reader

HID iCLASS® RW100: 6101CG40000, 6101CGM0000, 6101CK40000, 6101CK40002, 6101CK40100, 6101CK403C0, 6101CKM0000, 6101CKM0002, 6101CKM0203; RW300: 6111CG40000, 6111CG400C0, 6111CGM0000, 6111CK40000, 6111CK4000Z, 6111CKM0000; RW400: 6121CG40000, 6121CGM0000, 6121CK40000, 6121CK40003, 6121CK40007-G3.0, 6121CK4000D-G3.0, 6121CKM0000; R40: 6122CKP00P0, 6122CKP05P0, 6122CKP06P0; RWK400: 6131CG4020000, 6131CK4000000, 6131CK4000014, 6131CK4000300, 6131CK4020000, 6131CKM000000, 6131CKM000214; RK40: 6132BKP00Q709-G3.0, 6132CKP000009, 6132CKP000011, 6132CKP000700-G3.0, 6132CKP000709-G3.0, 6132CKP001009, 6132CKP001011, 6132CKP00P000, 6132CKP00P009, 6132CKP00P709-G3.0, 6132CKP00Q709-G3.0, 6132CKP030014, 6132CKP060514, 6132CKP06P009, 6132CKP06P609, 6132CKP070209; RW150: 6141CG40000, 6141CGM0000, 6141CK40000, 6141CKM00000; R15: 6142CKP000Z, 6142CKP00P0, 6142CKP0100; RWKL550: 6171BK4000000, 6171BK4000009, 6171BK4000014, 6171BK4000214, 6171BK4000500, 6171BK4040Z14, 6171BK4060000, 6171BK4060209, 6171BK4060Z09, 6171BK4061000, 6171BKM000000, 6171BKM000200, 6171BKM000300, 6171BKM040400; RWKLB575: 6181BK4000000, 6181BK4000009, 6181BK4000014, 6181BK4000022, 6181BK406C009; HID Smartid®: 8031DSAP

HID pivClass® R10-H: 900LHRNAK00000, 900LHRTAK00000, 900NHRNAK00000, 900NHRTAK00000, 900PHRNAK00000, 900PHRTAK00000, 910LHRNAK00000, 910LHRTAK00000, 910NHRNAK00000, 910NHRTAK00000, 910PHRNAK00000, 910PHRTAK00000, 920LHRNAK00000, 920LHRTAK00000, 920NHRNAK00000, 920NHRTAK00000, 920PHRNAK00000, 920PHRTAK00000, 921LHRNAK00000, 921LHRTAK00000, 921NHRNAK00000, 921NHRTAK00000, 921PHRNAK00000, 921PHRTAK00000; RPKCL40-P: 923LPRNAK00000, 923LPRTAK00000, 923NPRNAK00000, 923PPRNAK00000, 923PPRTAK00000

Aptiq™: M11, MTK15, MTMSK15, MT15, MTMS15

For information about which compatible RS485 access control readers have been verified by UL, see the Installation Guide available at www.axis.com

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:

- download user documentation and software updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrase
- report problems to Axis support staff by logging in to your private support area
- chat with Axis support staff (selected countries only)
- visit Axis Support at www.axis.com/techsup/

Learn More!

Visit Axis learning center www.axis.com/academy/ for useful trainings, webinars, tutorials and guides.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Table of Contents

Hardware Overview	5
LED Indicators	7
Connectors and Buttons	8
Access the Product	10
Access from a Browser	10
Access from the Internet	10
Set the Root Password	10
The Overview Page	11
System Configuration	12
Configuration – Step by Step	12
Select a Language	12
Configure the Hardware	13
Verify the Hardware Connections	17
Set the Date and Time	17
Configure the Network Settings	18
Configure Card Formats	19
Manage Network Door Controllers	21
Maintenance Instructions	23
Access Management	24
About Users	24
The Access Management Page	24
Choose a Workflow	24
Create and Edit Access Schedules	25
Create and Edit Groups	27
Manage Doors	27
Create and Edit Users	29
Example Access Schedule Combinations	31
Alarm and Event Configuration	33
View the Event Log	33
View the Alarm Log	33
Configure the Event and Alarm Logs	33
Set Up Action Rules	34
Reader Feedback	39
Reports	40
View, Print, and Export Reports	40
System Options	41
Security	41
Date & Time	43
Network	43
Ports & Devices	48
Maintenance	48
Support	49
Advanced	50
Reset to Factory Default Settings	50
Troubleshooting	51
Check the Firmware	51
Upgrade the Firmware	51
Emergency Recovery Procedure	51
Symptoms, Possible Causes and Remedial Actions	52
Technical Specifications	54
AXIS A1001 Network Door Controller	54
AXIS Entry Manager	56
Connectors	57
Connection Diagrams	61

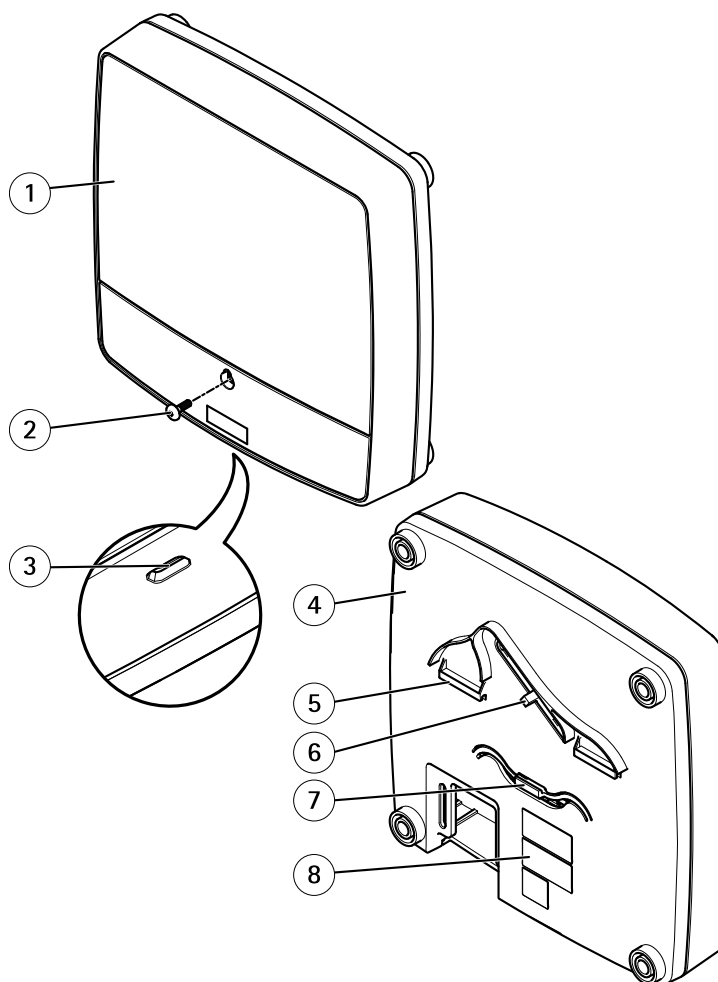
AXIS A1001 Network Door Controller & AXIS Entry Manager

Hardware Overview

Hardware Overview

The hardware overview is divided into the following categories:

- Front and back. See *page 5*.
- I/O interface. See *page 6*.
- External power inputs. See *page 6*.
- Power outputs. See *page 6*.
- LED indicators, buttons and other hardware. See *page 7*.

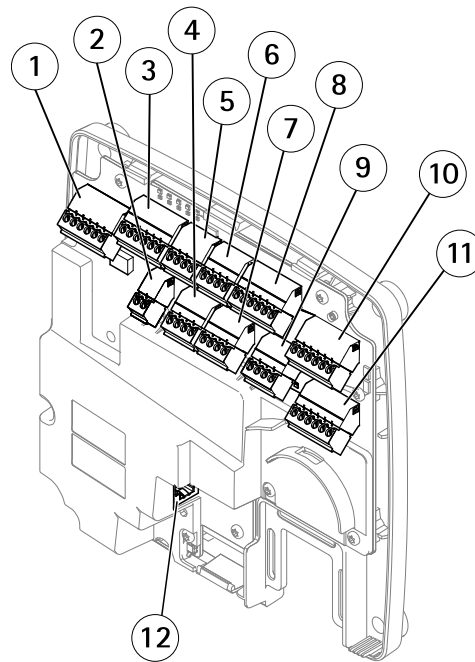


Front and back:

- 1 Cover
- 2 Cover screw
- 3 Cover removal slot
- 4 Base
- 5 DIN clip – upper
- 6 Tampering alarm switch – back
- 7 DIN clip – lower
- 8 Part number (P/N) & Serial number (S/N)

AXIS A1001 Network Door Controller & AXIS Entry Manager

Hardware Overview



I/O interface:

- 1 Reader data connector (READER DATA 1)
- 10 Reader data connector (READER DATA 2)
- 3 Reader I/O connector (READER I/O 1)
- 8 Reader I/O connector (READER I/O 2)
- 4 Door connector (DOOR IN 1)
- 7 Door connector (DOOR IN 2)
- 6 Auxiliary connector (AUX)
- 5 Audio connector (AUDIO) (not used)

External power inputs:

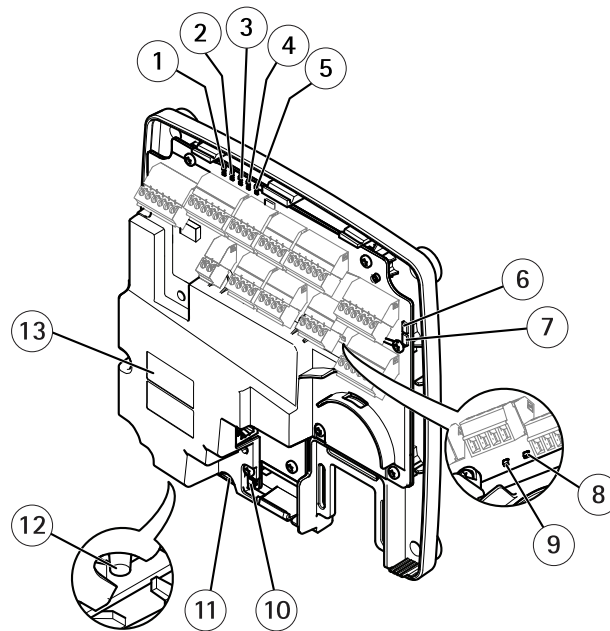
- 2 Power connector (DC IN)
- 12 Network connector (PoE)

Power outputs:

- 9 Power lock connector (LOCK)
- 11 Power & Relay connector (PWR, RELAY)

AXIS A1001 Network Door Controller & AXIS Entry Manager

Hardware Overview



LED indicators, buttons and other hardware:

- 1 Power LED indicator
- 2 Status LED indicator
- 3 Network LED indicator
- 4 Reader 2 LED indicator (not used)
- 5 Reader 1 LED indicator (not used)
- 6 Tampering alarm pin header – front (TF)
- 7 Tampering alarm pin header – back (TB)
- 8 Lock LED indicator
- 9 Lock LED indicator
- 10 Tampering alarm sensor – front
- 11 SD card slot (microSDHC) (not used)
- 12 Control button
- 13 Part number (P/N) & Serial number (S/N)

LED Indicators

LED	Color	Indication
Network	Green	Steady for connection to a 100 MBit/s network. Flashes for network activity.
	Amber	Steady for connection to a 10 MBit/s network. Flashes for network activity.
	Unlit	No network connection.
Status	Green	Steady green for normal operation.
	Amber	Steady during startup and when restoring settings.
	Red	Slow flash for failed upgrade.
Power	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Hardware Overview

Lock	Green	Steady when not energized.
	Red	Steady when energized.
	Unlit	Floating.

Note

- The Status LED can be configured to flash while an event is active.
- The Status LED can be configured to flash for identifying the unit. Go to **Setup > Additional Controller Configuration > System Options > Maintenance** .

Connectors and Buttons

For technical specifications, see *page 54*.

I/O Interface

Reader Data Connector

Two 6-pin terminal blocks supporting RS485 and Wiegand protocols for communication with the reader. For specifications, see *page 58*.

Reader I/O Connector

Two 6-pin terminal blocks for reader input and output. In addition to the 0 V DC reference point and power (DC output), the reader I/O connector provides the interface to:

- Digital input – For connecting, for example, reader tampering alarms.
- Digital output – For connecting, for example, reader beepers and reader LEDs.

For specifications, see *page 58*.

Door Connector

Two 4-pin terminal blocks for connecting door monitoring devices and request to exit (REX) devices. For specifications, see *page 59*.

Auxiliary Connector

4-pin configurable I/O terminal block. Use with external devices, in combination with, for example tampering alarms, event triggering and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

- Digital input – An alarm input for connecting devices that can toggle between an open and closed circuit, for example PIR sensors or glass break detectors.
- Digital output – For connecting external devices such as burglar alarms, sirens or lights. Connected devices can be activated by the VAPIX® application programming interface or by an action rule.

For specifications, see *page 59*.

External Power Inputs

NOTICE

The product shall be connected using a shielded network cable (STP). All cables connecting the product to the network shall be intended for their specific use. Make sure that the network devices are installed in accordance with the manufacturer's instructions. For information about regulatory requirements, see *Electromagnetic Compatibility (EMC) on page 2* .

Power Connector

2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤ 100 W or a rated output current limited to ≤ 5 A. For specifications, see *page 59*.

Network Connector

RJ45 Ethernet connector. Supports Power over Ethernet (PoE). For specifications, see *page 60*.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Hardware Overview

Power Outputs

Power Lock Connector

4-pin terminal block for connecting one or two locks. The lock connector can also be used to power external devices. For specifications, see *page 60*.

Power & Relay Connector

6-pin terminal block for connecting power and the door controller's relay to external devices such as locks and sensors. For specifications, see *page 60*.

Buttons and Other Hardware

Tampering Alarm Pin Header

Two 2-pin headers for disconnecting the front and back tampering alarms. For specifications, see *page 60*.

Control Button

The control button is used for:

- Resetting the product to factory default settings. See *page 50*.
- Connecting to an AXIS Video Hosting System service. See *page 45*. To connect, press and hold the button for about 1 second until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service. See *page 45*. To connect, press and hold the button for about 3 seconds.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access the Product

Access the Product

To install the Axis product, refer to the Installation Guide supplied with the product.

The product can be used with most operating systems and browsers. The recommended browsers are Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See *Technical Specifications on page 54*

Access from a Browser

1. Start a browser (Chrome, Internet Explorer, Firefox, Safari).
2. Enter the IP address or host name of the Axis product in the browser's Location/Address field. To access the product from a Macintosh computer (Mac OS X), click on the Bonjour tab and select the product from the drop-down list.

If you do not know the IP address, use AXIS IP Utility to locate the product on the network. For information about how to discover and assign an IP address, see the support pages at www.axis.com/techsup or the Installation Guide available at www.axis.com

3. Enter your user name and password. If this is the first time the product is accessed, the root password must first be configured. For instructions, see *Set the Root Password on page 10*.
4. AXIS Entry Manager opens in your browser. The start page is called the Overview page.

Access from the Internet

Once connected, the Axis product is accessible on your local network (LAN). To access the product from the Internet you must configure your network router to allow incoming data traffic to the product. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the product. This is enabled from **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

For more information, see *NAT traversal (port mapping) for IPv4 on page 46*. See also AXIS Internet Dynamic DNS Service at www.axiscam.net

For Technical notes on this and other topics, visit the Axis Support web at www.axis.com/techsup

Set the Root Password

To access the Axis product, you must set the password for the default administrator user **root**. This is done in the **Configure Root Password** dialog, which opens when the product is accessed for the first time.

To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate. HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information. See *HTTPS on page 41*.

The default administrator user name **root** is permanent and cannot be deleted. If the password for root is lost, the product must be reset to the factory default settings. See *Reset to Factory Default Settings on page 50*.

To set the password via a standard HTTP connection, enter it directly in the dialog.

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click **Use HTTPS**.
A temporary certificate (valid for one year) is created, enabling encryption of all traffic to and from the product, and the password can now be set securely.
2. Enter a password and then re-enter it to confirm the spelling.
3. Click **OK**. The password has now been configured.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access the Product

The Overview Page

The Overview page in AXIS Entry Manager shows information about the door controller's name, MAC address, IP address, and firmware version. It also enables you to identify the door controller on the network or in the system.

The first time you access the Axis product, the Overview page will prompt you to configure the hardware, to set date and time, to configure the network settings, and to configure the door controller as part of a system or as a standalone unit. For more information about configuring the system, see *Configuration – Step by Step on page 12*.

To return to the Overview page from the product's other webpages, click **Overview** in the menu bar.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

System Configuration

To open the product's Setup pages, click **Setup** in the top right-hand corner of the Overview page.

The Axis product can be configured by administrators. For more information about users and administrators, see *page 24*, *page 29*, and *page 41*.

Configuration – Step by Step

Before you start using the access control system, you should complete the following setup steps:

1. If English is not your first language, you may want AXIS Entry Manager to use a different language. See *Select a Language on page 12*.
2. Configure the door controller and connected devices such as readers, locks and request to exit (REX) devices. See *Configure the Hardware on page 13*.
3. Verify the Hardware Connections. See *page 17*.
4. Set the date and time. See *page 17*.
5. Configure the network settings. See *page 18*.
6. Configure card formats. See *page 19*.
7. Configure the door controller system. See *Manage Network Door Controllers on page 21*.

For information about how to configure and manage the system's doors, schedules, users and groups, see *Access Management on page 24*.

For information about maintenance recommendations, see *Maintenance Instructions on page 23*.


Note

To add or remove door controllers, to add, remove, or edit users, or to configure the hardware, more than half of the door controllers in the system must be **online**. To check the door controller status, go to **Setup > Manage Network Door Controllers in System**.

Select a Language

The default language of AXIS Entry Manager is English, but you can switch to any of the languages that are included in the product's firmware. For information about the latest available firmware, see www.axis.com

You can switch languages in any of the product's webpages.

To switch languages, click the language drop-down list  and select a language. All the product's webpages and help pages are displayed in the selected language.

Important

- Language selection is supported from firmware 1.25. If the door controller uses an earlier version, you need to upgrade the firmware before you can select a language. See *Upgrade the Firmware on page 51*.
- Language settings are not shared between door controllers in the system. Either select the language in all door controllers, or always open Axis Entry Manager from the same door controller.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

Note

- When you switch languages, the date format also changes to a format commonly used in the selected language. The correct format is displayed in the data fields.
- If you reset the product to factory default settings, AXIS Entry Manager switches back to English.
- If you restore the product, AXIS Entry Manager will continue to use the selected language.
- If you restart the product, AXIS Entry Manager will continue to use the selected language.
- If you upgrade the firmware, AXIS Entry Manager will continue to use the selected language.

Configure the Hardware

Before you can manage the doors, the hardware must be configured in the Hardware Configuration pages.

Doors, locks and other devices can be connected to the Axis product before completing the hardware configuration. However, the connection of devices will be easier if you complete the hardware configuration first. This is because the hardware pin chart will be available when the configuration is complete. The hardware pin chart is a guide on how to connect the pins and can be used as a reference sheet for maintenance. For maintenance instructions, see *page 23*.

If configuring the hardware for the first time, select one of the following methods:

- Import a hardware configuration file. See *page 13*.
- Create a new hardware configuration. See *page 14*.

Import a Hardware Configuration File

The hardware configuration of the Axis product can be completed faster by importing a hardware configuration file.

By exporting the file from one product and importing it to others, you can make multiple copies of the same hardware setup without having to repeat the same steps over and over again. You can also store exported files as backups and use them to restore previous hardware configurations. For more information, see *Export a Hardware Configuration File on page 13*.

To import a hardware configuration file:

1. Go to **Setup > Hardware Configuration**.
2. Click **Import hardware configuration** or, if there a hardware configuration already exists, **Reset and import hardware configuration**.
3. In the file browser dialog that appears, locate and select the hardware configuration file (*.json) on your computer.
4. Click **OK**.

Export a Hardware Configuration File

The hardware configuration of the Axis product can be exported to make multiple copies of the same hardware setup. You can also store exported files as backups and use them to restore previous hardware configurations.

To export a hardware configuration file:

1. Go to **Setup > Hardware Configuration**.
2. Click **Export hardware configuration**.
3. Depending on the browser, you may need to go through a dialog to complete the export.

Unless otherwise specified, the exported file (*.json) is saved in the default download folder. You can select a download folder in the web browser's user settings.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

Create a New Hardware Configuration

To create a new hardware configuration from the beginning:

1. Go to **Setup > Hardware Configuration** and click **Start new hardware configuration**.
If the product's hardware has not been configured before or has been deleted, **Hardware Configuration** will be available in the notification panel in the Overview page.
2. Select a door option depending on the number of doors, one (1) or two (2), that will be connected to the Axis product.
3. Enter a descriptive name for each door and click **Next**. It is recommended to provide the doors with unique descriptive names so that they easily can be identified by anyone who will administrate the system.
You can also edit the name of the Axis product. The default name includes the serial number for easy identification.
4. Select the door monitor and lock options that match the requirements and the type of lock connections that will be used and click **Next**. For more information, see *Configure Locks and Door Monitors on page 14* and *Lock Options on page 15*.
5. Select the types of readers that will be used and click **Finish**. For more information, see *Configure Readers and REX Devices on page 16* and *Reader and REX Device Options on page 16*.
6. In the dialog that appears after completing the configuration, click **OK** or click the link to view the hardware pin chart.
To print the hardware pin chart, click **Print Hardware Pin Chart** on the Hardware Pin Chart page.

To cancel the hardware configuration, click **Cancel**. This can be done in any of the hardware configuration pages.

Configure Locks and Door Monitors

1. If a door monitor will be used, select **Door monitor** and then select the option that matches how the door monitor circuits will be connected.
2. If the door lock shall lock immediately after the door has been opened, select **Cancel access time once door is opened**.
3. Specify the door monitor time options or, if no door monitor will be used, the lock time options.
4. Select the options that match how the lock circuits will be connected.
5. If a lock monitor will be used, select **Lock monitor** and then select the options that match how the lock monitor circuits will be connected.
6. If the input connections from readers, REX devices, and door monitors shall be supervised, select **Enable supervised inputs**.
For more information, see *Use Supervised Inputs on page 16*.

Note

- Most lock, door monitor, and reader options can be changed without resetting and starting a new hardware configuration. Go to **Setup > Hardware Reconfiguration**.
- You can connect one lock monitor per door controller. So if you use double-lock doors, only one of the locks can have a lock monitor. If two doors are connected to the same door controller, lock monitors cannot be used.
- Motorized locks must be configured as secondary locks.

Door Monitor Options

The following door monitor options are available:

- **Door monitor** – Selected by default. Each door has its own door monitor that, for example, will signal when the door has been forced open or open too long. Deselect if no door monitor will be used.
 - **Open circuit = Closed door** – Select if the door monitor circuit is normally open. The door monitor gives the door open signal when the circuit is closed. The door monitor gives the door closed signal when the circuit is open.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

- **Open circuit = Open door** – Select if the door monitor circuit is normally closed. The door monitor gives the door open signal when the circuit is open. The door monitor gives the door closed signal when the circuit is closed.
- **Cancel access time once door is opened** – Select to prevent tailgating, that is, stop unauthorized visitors from accessing the door. The door will lock immediately after the door has been opened. When the door closes, the door will be locked and cannot be opened until a user requests and is granted access again.

The following door monitor time options are available:

- **Access time** – Set the number of seconds the door shall remain unlocked after access has been granted. The door remains unlocked until the door has been opened and will lock when it closes regardless of whether the access time has expired or not. If the door remains unopened, it locks when the set access time has been reached.
- **Open too long time** – Set the number of seconds the door is allowed to stay open. If the door is still open when the open too long time has been reached, the door open too long alarm is triggered. Set up an action rule to configure which action the open too long event shall trigger.
- **Pre-alarm time** – A pre-alarm is a warning signal that is triggered before the open too long time has been reached. It tells the administrator and, depending on how the action rule has been set up, it can also warn the user (the person entering the door) that the door needs to be closed or the real alarm, the door open too long alarm, will go off. Set the number of seconds before the door open too long alarm is triggered the system shall give the pre-alarm warning signal. To disable the pre-alarm, set the pre-alarm time to 0.

For information about how to set up an action rule, see *Set Up Action Rules on page 34*.

Lock Options

Deselect **Door monitor** to make the following lock time options available:

- **Door unlocked time** – Set the number of seconds the door shall remain unlocked after access has been granted. The door remains unlocked until the door has been opened and will lock when it closes regardless of whether the door unlocked time has expired or not. If the door remains unopened, it locks when the set door unlock time has been reached.
- **Pre-lock signal time** – A pre-lock signal is a warning signal that is triggered before the door locks. It tells the administrator and, depending on how the action rule has been set up, it can also warn the user (the person entering the door) that the door will lock soon. Set the number of seconds before the door locks the system shall give the pre-lock warning signal. The pre-lock signal time must be shorter than the door unlocked time. To disable the pre-lock warning signal, set the pre-lock signal time to 0.

The following lock circuit options are available:

- **12 V**
 - **Fail-secure** – Select for locks that remain locked during power outages. When applying electric current, the lock will unlock.
 - **Fail-safe** – Select for locks that unlock during power outages. When applying electric current, the lock will lock.
- **Relay** – Can only be used on one lock per door controller. If two doors are connected to the door controller, a relay can only be used on the lock of the second door.
 - **Relay open = Locked** – Select for locks that remain locked when the relay is open (fail-secure). When the relay closes, the lock will unlock.
 - **Relay open = Unlocked** – Select for locks that unlock during power outages (fail-safe). When the relay closes, the lock will lock.
- **None** – Select if only one lock will be used.

The following lock monitor options are available:

- **Lock monitor** – Select to make the lock monitor controls available. Then select the lock that shall be monitored. A lock monitor can only be used on double-lock doors and cannot be used if two doors are connected to the door controller.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

- **Open circuit = Locked** – Select if the lock monitor circuit is normally closed. The lock monitor gives the door unlocked signal when the circuit is closed. The lock monitor gives the door locked signal when the circuit is open.
- **Open circuit = Unlocked** – Select if the lock monitor circuit is normally open. The lock monitor gives the door unlocked signal when the circuit is open. The lock monitor gives the door locked signal when the circuit is closed.

For information about how to set up an action rule, see *Set Up Action Rules on page 34*.

Configure Readers and REX Devices

1. If a reader will be used, select **Reader** and then select the options that match the reader's communication protocol.
2. If a request to exit (REX) device such as a button, sensor, or push bar will be used, select **REX** and then select the option that matches how the REX device's circuits will be connected.

If the door shall remain locked until the user manually unlocks and opens the door, select **REX does not unlock door**.
3. If connecting more than one reader or REX device to the door controller, do the previous two steps again until each reader or REX device has the correct settings.

Reader and REX Device Options

The following reader options are available:

- **Wiegand** – Select for readers that use Wiegand protocols. Then select the LED control that is supported by the reader. Readers with single LED control usually toggle between red and green. Readers with dual LED control use different wires for the red and green LEDs. This means that the LEDs are controlled independently of each other. When both LEDs are on, the light appears to be amber. See the manufacturer's information about which LED control the reader supports.
- **RS485 half duplex** – Select for RS485 readers with half duplex support. Then select the RS485 protocol that is supported by the reader. See the manufacturer's information about which protocol the reader supports.
- **RS485 full duplex** – Select for RS485 readers with full duplex support. Then select the RS485 protocol that is supported by the reader. See the manufacturer's information about which protocol the reader supports.

The following REX device options are available:

- **Active low** – Select if activating the REX device closes the circuit.
- **Active high** – Select if activating the REX device opens the circuit.
- **REX does not unlock door** – Select if the door shall remain locked until the user manually unlocks and opens the door. The door forced open alarm will not be triggered as long as the user opens the door within the access time. Deselect if the door shall unlock automatically when the user activates the REX device.

Important

If the door controller has only been configured with one door before it is upgraded to firmware 1.15 or later from firmware 1.10, **REX does not unlock door** will be non-selectable at first. To make **REX does not unlock door** selectable, go to **Setup > Hardware Configuration** and click **Reset and start a new hardware configuration**. Then set up the rules for the doors connected to the door controller and add them to groups, see *Manage Doors*.

Note

Most lock, door monitor, and reader options can be changed without resetting and starting a new hardware configuration. Go to **Setup > Hardware Reconfiguration**.

Use Supervised Inputs

Supervised inputs report on the status of the connection between the door controller and the readers, REX devices, and door monitors. If the connection is interrupted, an event is activated.

To use supervised inputs:

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

1. Install end of line resistors on all the used inputs. See the connection diagram on *page 62*.
2. Go to **Setup > Hardware Reconfiguration** and select **Enable supervised inputs**. You can also enable supervised inputs during the hardware configuration.

Supervised Input Compatibility

The following connectors support supervised inputs:

- Reader I/O connector – tampering signal. See *page 58*.
- Door connector. See *page 59*.

Readers and switches that can be used with supervised inputs include:

- HID readers with internal 1 k Ω pull-up to 5 V.
- Readers and switches with internal 1 k Ω pull-up to 5 V.
- Readers and switches without internal pull-up.

Verify the Hardware Connections

When the hardware installation and configuration is complete, and anytime during the door controller's lifetime, you can verify the function of the connected door monitors, locks and readers.

To verify the configuration and access the verification controls, go to **Setup > Hardware Connection Verification**.

Verification Controls

- **Door state** – Verify the current state of the door monitor, door alarms and locks. Click **Get current state**.
- **Lock** – Manually trigger the lock. Both primary locks and secondary locks if there are any will be affected. Click **Lock or Unlock**.
- **Lock** – Manually trigger the lock to grant access. Only primary locks will be affected. Click **Access**.
- **Reader: Feedback** – Verify the reader feedback, for example sounds and LED signals, for different commands. Select the command and click **Test**. Which types of feedback that are available depends on the reader. For more information, see *Reader Feedback*. See also the manufacturer's instructions.
- **Reader: Tampering** – Get information about the last tampering attempt. The first tampering attempt will be registered when the reader is installed. Click **Get last tampering**.
- **Reader: Card swipe** – Get information about the last swiped card or other type of user token accepted by the reader. Click **Get last credential**.
- **REX** – Get information about the last time the request to exit (REX) device was pressed. Click **Get last REX**.

Set the Date and Time

If the door controller is part of a system, the date and time settings will be distributed to all the door controllers. This means that the settings are pushed to the other controllers in the system, regardless of whether you synchronize with an NTP server, set the date and time manually, or get the date and time from the computer. If you cannot see the changes, try refreshing the page in your browser. For more information about managing a system of door controllers, see *Manage Network Door Controllers on page 21*.

To set the date and time of the Axis product, go to **Setup > Date & Time**.

You can set the date and time in the following ways:

- Get the date and time from a network time protocol (NTP) server. See *page 18*.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

- Set the date and time manually. See *page 18*.
- Get the date and time from the computer. See *page 18*.

Current controller time displays the door controller's current date and time (24h clock).

The same options for date and time are also available in the System Options pages. Go to **Setup > Additional Controller Configuration > System Options > Date & Time**.

Get the Date and Time from a Network Time Protocol (NTP) Server

1. Go to **Setup > Date & Time**.
2. Select your **Timezone** from the drop-down list.
3. If daylight saving time is used in your region, select **Adjust for daylight saving** .
4. Select **Synchronize with NTP**.
5. Select the default DHCP address or enter the address of a NTP server.
6. Click **Save**.

When synchronizing with an NTP server, date and time are updated continuously because the data is pushed from the NTP server. For information about NTP settings, see *NTP Configuration on page 45*.

If you use a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 45*.

Set the Date and Time Manually

1. Go to **Setup > Date & Time**.
2. If daylight saving time is used in your region, select **Adjust for daylight saving** .
3. Select **Set date & time manually**.
4. Enter the desired date and time.
5. Click **Save**.

When setting the date & time manually, date and time are set once and will not be updated automatically. This means that if the date or time needs to be updated, the changes must be made manually because there is no connection to an external NTP server.

Get the Date and Time from the Computer

1. Go to **Setup > Date & Time**.
2. If daylight saving time is used in your region, select **Adjust for daylight saving** .
3. Select **Set date & time manually**.
4. Click **Sync now and save**.

When using the computer time, date and time are synchronized with the computer time once and will not be updated automatically. This means that if you change the date or time on the computer you use to manage the system, you should synchronize again.

Configure the Network Settings

To configure the basic network settings, go to **Setup > Network Settings** or to **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic**.

For more information about network settings, see *Network on page 43*.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

Basic TCP/IP Settings

The Axis product supports IP version 4 (IPv4).

The Axis product can get an IPv4 address in the following ways:

- **Dynamic IP address – Obtain IP address via DHCP** is selected by default. This means that the Axis product is set to get the IP address automatically via Dynamic Host Configuration Protocol (DHCP).
DHCP allows network administrators to centrally manage and automate the assignment of IP addresses.
- **Static IP address** – To use a static IP address, select **Use the following IP address** and specify the IP address, subnet mask and default router. Then click **Save**.

DHCP should only be enabled when using dynamic IP address notification, or if the DHCP can update a DNS server that makes it possible to access the Axis product by name (host name).

If DHCP is enabled and the product cannot be accessed, run **AXIS IP Utility** to search the network for connected Axis products, or reset the product to the factory default settings and then perform the installation again. For information about how to reset to factory default, see *page 50*.

Configure Card Formats


The door controller has a few predefined commonly used card formats that you can use as they are or modify as required. You can also create custom card formats. Each card format has a different set of rules, field maps, for how the information stored on the card is organized. By defining a card format you tell the system how to interpret the information that the readers get from cards and other tokens. For information about which card formats the reader supports, see the manufacturer's instructions.


To enable card formats:

1. Go to **Setup > Configure Card Formats**.
2. Select one or more card formats that match the card format used by the connected readers.


To create new card formats:

1. Go to **Setup > Configure Card Formats**.
2. Click **Add card format**.
3. In the **Add card format** dialog, enter a name, a description, and the bit length of the card format. See *Card Format Descriptions on page 20*.
4. Click **Add field map** and enter the required information in the fields. See *Field Maps on page 20*.
5. To add multiple field maps, repeat the previous step.

To expand an item in the **Card formats** list and view the card format descriptions and field maps, click .

To edit a card format, click  and change the card format descriptions and field maps as required. Then click **Save**.

To delete a field map in the **Edit card format** or **Add card format** dialog, click .

To delete a card format, click .

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

Important

- All changes to card formats apply to the whole system of door controllers.
- You can only enable and disable card formats if at least one door controller in the system has been configured with at least one reader. See *Configure the Hardware on page 13* and *Configure Readers and REX Devices on page 16*.
- Two card formats with the same bit length cannot be active the same time. For example, if you have defined two 32-bit card formats, "Format A" and "Format B", and you have enabled "Format A", you cannot enable "Format B" without disabling "Format A" first.
- If no card formats have been enabled, you can use the **Card raw only** and **Card raw and PIN** identification types to identify a card and grant access to users.

Card Format Descriptions

- **Name (required)** – Enter a descriptive name.
- **Description** – Enter additional information as desired. This information is only visible in the **Edit card format** and **Add card format** dialogs.
- **Bit length (required)** – Enter the bit length of the card format. This has to be a number between 1 and 1000000000.

Field Maps

- **Name (required)** – Enter the field map name unspaced, for example `OddParity`.

Examples of common field maps include:

- `Parity` – Parity bits are used for error detection. Parity bits are usually added to the beginning or end of a binary code string and indicate if the number of bits is even or odd.
 - `EvenParity` – Even parity bits make sure that there is an even number of bits in the string. The bits that have the value 1 are counted. If the count is already even, the parity bit value is set to 0. If the count is odd, the even parity bit value is set to 1, making the total count an even number.
 - `OddParity` – Odd parity bits make sure that there is an odd number of bits in the string. The bits that have the value 1 are counted. If the count is already odd, the odd parity bit value is set to 0. If the count is even, the parity bit value is set to 1, making the total count an odd number.
 - `FacilityCode` – Facility codes are sometimes used for verifying that the token matches the facility's access control system. Often all tokens issued for a single facility have the same facility code.
 - `CardNr` – The card number binary data is encoded as integer numbers in either little endian byte order (`BinLE2Int`) or big endian byte order (`BinBE2Int`). See below.
 - `CardNrHex` – The card number binary data is encoded as hex-lowercase numbers in either little endian byte order (`BinLE2hex`) or big endian byte order (`BinBE2hex`). See below.
- **Range (required)** – Enter the bit range of the field map, for example 1, 2–17, 18–33, and 34.
 - **Encoding (required)** – Select the encoding type of each field map.
 - `BinLE2Int` – Binary data is encoded as integer numbers in little endian byte order. Integer means that it needs to be a whole number (no decimals). Little endian byte order means that in a multiple-byte sequence, the first byte is the smallest.
 - `BinBE2Int` – Binary data is encoded as integer numbers in big endian byte order. Integer means that it needs to be a whole number (no decimals). Big endian byte order means that in a multiple-byte sequence, the first byte is the biggest.
 - `BinLE2Hex` – Binary data is encoded as hex-lowercase numbers in little endian byte order. The hexadecimal system, also known as the base-16 number system, consists of 16 unique symbols: the numbers 0–9 and the letters a–f. Little endian byte order means that in a multiple-byte sequence, the first byte is the smallest.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

- **BinBE2Hex** – Binary data is encoded as hex-lowercase numbers in big endian byte order. The hexadecimal system, also known as the base-16 number system, consists of 16 unique symbols: the numbers 0–9 and the letters a–f. Big endian byte order means that in a multiple-byte sequence, the first byte is the biggest.

For information about which field maps your card format uses, see the manufacturer's instructions.

Manage Network Door Controllers

The Manage Network Door Controllers in System page shows information about the door controller, its system status, and which other door controllers are part of the system. It also enables the administrator to change the system setup by adding and removing door controllers.

To manage door controllers, go to **Setup > Manage Network Door Controllers in System**.

The Manage Network Door Controllers in System page includes the following panels:

- **System status of this controller** – Shows the door controller's system status and enables switching between system and standalone modes. For more information, see *Door Controller System Status on page 21*.
- **Network door controllers in system** – Shows information about the door controllers in the system and includes controls for adding and removing a controller from the system. For more information, see *Connected Door Controllers in the System on page 21*.

Door Controller System Status

If the door controller can be part of a system of door controllers depends on its system status. The door controller's system status is displayed in the **System status for this controller** panel.

If the door controller is not in standalone mode and you want to protect the door controller from being added to a system, click **Activate standalone mode** to enter standalone mode.

If the door controller is in standalone mode but you intend to add the door controller to a system, click **Deactivate standalone mode** to leave the standalone mode.

System Modes

- **This controller is not part of a system and not in standalone mode** – The door controller has not been configured as part of a system and it is not in standalone mode. This means that the door controller is open and can be added to a system by any other door controller within the same network. To protect the door controller from being added to a system, activate the standalone mode.
- **This controller is set to standalone mode** – The door controller is not part of a system. It cannot be added to a system by other door controllers in the network or add other door controllers itself. Standalone mode is typically used in small setups with one door controller and one or two doors. To allow the door controller to be added into a system, deactivate the standalone mode.
- **This controller is part of a system** – The door controller is part of a distributed system. In the distributed system, users, groups, doors, and schedules are shared between the connected controllers.

Connected Door Controllers in the System

The **Network door controllers in system** panel provides controls for the following system changes:

- Add a door controller to a system, see *Add Door Controllers to the System on page 22*.
- Remove a door controller from a system, see *Remove Door Controllers from the System on page 22*.

Connected Door Controllers List

The **Network door controllers in system** panel also includes a list that shows the following ID and status information about the connected door controllers in the system:

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

- **Name** – The user-defined name of the door controller. If the administrator has not set a name when configuring the hardware, the default name will be shown.
- **IP address**
- **MAC address**
- **Status** – The door controller from which you access the system will show status **This controller**. The other door controllers in the system will show status **Online**.

To open the webpages of another door controller, click the controller's IP address.

To update the list, click **Refresh the list of controllers**.

Add Door Controllers to the System

Important

When pairing door controllers, all access management settings on the added door controller will be deleted and overwritten by the system's access management settings.

To add a door controller to the system from the list of door controllers:

1. Go to **Setup > Manage Network Door Controllers in System**.
2. Click **Add controllers to system from list**.
3. Select the door controller that you wish to add.
4. Click **Add**.
5. To add more door controllers, repeat the steps above.

To add a door controller to the system by its known IP address or MAC address:

1. Go to **Manage Devices**.
2. Click **Add controller to system by IP or MAC address**.
3. Enter the IP address or MAC address.
4. Click **Add**.
5. To add more door controllers, repeat the steps above.

When the pairing is completed, all users, doors, schedules, and groups are shared by all door controllers in the system.

To update the list, click **Refresh list of controllers**.

Remove Door Controllers from the System

Important

- Before removing a door controller from the system, reset its hardware configuration. If you skip this step, all doors related to the removed door controller will remain in the system and cannot be deleted.
- When removing a door controller from a two-controller system, both door controllers automatically switch to standalone mode.

To remove a door controller from the system:

1. Access the system through the door controller that you want to remove and go to **Setup > Hardware Configuration**.
2. Click **Reset hardware configuration**.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Configuration

3. After the hardware configuration has been reset, go to **Setup > Manage Network Door Controllers in System**.
4. In the **Network door controllers in system** list, identify the door controller that you want to remove and click **Remove from system**.
5. A dialog opens reminding you to reset the door controller's hardware configuration. Click **Remove controller** to confirm.
6. A dialog opens prompting you to confirm that you want to remove the door controller. Click **OK** to confirm. The removed door controller is now in standalone mode.

Note

- When a door controller is removed from the system, all its access management settings are deleted.
- Only door controllers that are online can be removed.

Maintenance Instructions

To keep the access control system running smoothly, Axis recommends regular maintenance of the access control system, including door controllers and connected devices.

Do maintenance at least once a year. The suggested maintenance procedure includes, but is not limited to, the following steps:

- Make sure all the connections between the door controller and the external devices are secure.
- Verify all the hardware connections. See *Verification Controls on page 17*.
- Verify that the system, including the connected external devices, functions correctly.
 - Swipe a card and test the readers, doors, and locks.
 - If the system includes REX devices, sensors or other devices, test them as well.
 - If activated, test the tampering alarms.

If the results from any of the steps above indicate faults or unexpected behavior:

- Test the signals of the wires using appropriate equipment and check if the wires or cables are damaged in any way.
- Replace all damaged or faulty cables and wires.
- Once the cables and wires have been replaced, verify all the hardware connections again. See *Verification Controls on page 17*.
- Make sure all access schedules, doors, groups, and users are up to date.
- If the door controller is not behaving as expected, see *Troubleshooting on page 51* and *Maintenance on page 48* for more information.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management

Access Management

About Users

In AXIS Entry Manager, users are people who have been registered as owners of one or more tokens (identification types). Each person must have a unique user profile to be granted access to doors in the access control system. The user profile consists of credentials that tell the system who the user is and when and how they are granted access to doors. For more information, see *Create and Edit Users on page 29*.

Users in this context should not be confused with administrators. Administrators have unrestricted access to all settings. And in the context of managing the access control system, the product's web pages (AXIS Entry Manager), administrators are also sometimes referred to as users. For more information, see *Users on page 41*.

The Access Management Page

The Access Management page allows you to configure and manage the system's users, groups, doors, and schedules. To open the Access Management page, click **Access Management**.

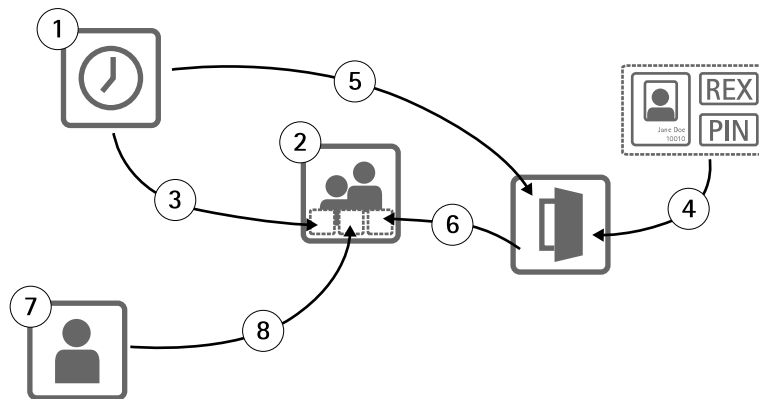
To add users to groups and apply access schedules and doors, drag the items to their respective destination in the **Groups** and **Doors** lists.

Note

Messages that require action are shown in red text.

Choose a Workflow

The access management structure is flexible, allowing you to develop a workflow that suits your needs. The following is a workflow example:



1. Create access schedules. See *page 25*.
2. Create groups. See *page 27*.
3. Apply access schedules to groups.
4. Add identification types to doors. See *page 27* and *page 28*.
5. Apply access schedules to each identification type.
6. Apply doors to groups.
7. Create users. See *page 29*.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management

8. Add users to groups.


For applied examples of this workflow, see *Example Access Schedule Combinations on page 31*.


Create and Edit Access Schedules

Access schedules are used to define general rules for when doors can and cannot be accessed. They are also used to define rules for when groups can and cannot access the doors in the system. For more information, see *Access Schedule Types on page 25*.


To create a new access schedule:

1. Go to **Access Management**.
2. In the **Access Schedules** tab, click **Add new schedule**.
3. In the **Add access schedule** dialog, enter the schedule name.
4. To create a regular access schedule, select **Addition Schedule**.
Or to create a subtraction schedule, select **Subtraction Schedule**.
For more information, see *Access Schedule Types*.
5. Click **Save**.

To expand an item in the **Access Schedules** list, click . Addition schedules are shown in green text and subtraction schedules are shown in dark red text.

To view an access schedule's calendar, click .

To edit an access schedule's name or a schedule item, click  and make the changes. Then click **Save**.

To delete an access schedule, click .

Note

The door controller has a few predefined commonly used access schedules that can be used as examples or modified as required. However, the predefined access schedule **Always** cannot be modified or deleted.

Access Schedule Types

There are two types of access schedules:

- **Addition schedule** – Regular access schedules that define when doors can be accessed. Typical addition schedules are office hours, business hours, after hours, or night time hours.
- **Subtraction schedule** – Exceptions to regular access schedules. They are generally used to restrict access during a specific time period that occurs within the time period of a regular schedule (addition schedule). For example, subtraction schedules can be used to deny users access to the building during public holidays that occur on weekdays.

Both types of access schedules can be used at two levels:

- **Identification type schedules** – Determine when and how readers grant users access to a door. Each identification type must be connected to an access schedule that tells the system when to grant users access with that particular identification type. Multiple addition schedules and subtraction schedules can be added to each identification type. For information about identification types, see *page 28*.
- **Group schedules** – Determine when, but not how, members of a group are granted access to a door. Each group must be connected to one or more access schedules that tell the system when to grant its members access. Multiple addition schedules and subtraction schedules can be added to each group. For information about groups, see *page 27*.

Group schedules can restrict entry access rights but not extend entry or exit access rights beyond what the identification type schedules allow. In other words, if an identification type schedule restricts entry or exit access at certain times, a group schedule

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management

cannot override that identification type schedule. However, if a group schedule is more restrictive about access than the identification type schedule, the group schedule overrides the identification type schedule.

Identification type schedules and group schedules can be combined in several ways to achieve different results. For example access schedule combinations, see *page 31*.

Add Schedule Items

Both addition schedules and subtraction schedules can be one-time (single) events or recurring events.

To add a schedule item to an access schedule:

1. Expand the access schedule in the **Access Schedules** list.
2. Click **Add schedule item**.
3. Enter the name of the scheduled item.
4. Select **One time** or **Recurrence**.
5. Set the duration in the time fields. See *Time Options*.
6. For recurring schedule events, select the **Recurrence pattern** and **Range of recurrence parameters**. See *Recurrence Pattern Options* and *Range of Recurrence Options*.
7. Click **Save**.

Time Options

The following time options are available:

- **All day** – Select for events that last for all 24 hours of the day. Then enter the desired **Start** date.
- **Start** – Click the time field and select the desired time. If required, click the date field and select the desired month, day, and year. You can also type the date directly in the field.
- **End** – Click the time field and select the desired time. If required, click the date field and select the desired month, day, and year. You can also type the date directly in the field.

Recurrence Pattern Options

The following recurrence pattern options are available:

- **Yearly** – Select to repeat every year.
- **Weekly** – Select to repeat every week.
- **Rekurs every week on Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday** – Select which days to repeat.

Range of Recurrence Options

The following range of recurrence options are available:

- **First occurrence** – Click the date field and select the desired month, day, and year. You can also type the date directly in the field.
- **No end date** – Select to repeat the occurrence indefinitely.
- **End by** – Click the date field and select the desired month, day, and year. You can also type the date directly in the field.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management


Create and Edit Groups

Groups allow you to manage users and their access rights collectively and efficiently. A group consists of credentials that tell the system which users the group consists of and when and how the group members are granted access to the doors.


Each user must belong to one or more groups. To add a user to a group, drag and drop the user to the desired group in the **Groups** list. For more information, see *Create and Edit Users on page 29*.


To create a new group:

1. Go to **Access Management**.
2. In the **Groups** tab, click **Add new group**.
3. In the **Add Group** dialog, enter the group's credentials. See *Group Credentials on page 27*.
4. Click **Save**.

To expand an item in the **Groups** list and view its members, door access rights and schedules, click .

To edit a group's name or validity date, click  and make the changes. Then click **Save**.

To verify when and how a group can access certain doors, click .

To delete a group or group members, doors or schedules from a group, click .

Group Credentials

The following credentials are available for groups:

- **Name** (required)
- **Valid from** and **Valid to** – Enter the dates between which the group's credentials shall be valid. Click the date field and select the desired month, day, and year. You can also type the date directly in the field.

Note


To be able to save the profile, you must enter the group's **Name**.

Manage Doors

The general rules for each door are managed in the **Doors** tab. The rules include adding identification types that determine how users will be granted access to the door and access schedules that determine when each identification type is valid. For more information, see *Identification Types on page 28* and *Create and Edit Access Schedules on page 25*.

Before you can manage a door, you must add it to the access control system by completing the hardware configuration, see *Configure the Hardware on page 13*.

To manage a door:

1. Go to **Access Management** and select the **Doors** tab.
2. In the **Doors** list, click  next to the door you want to edit.
3. Drag the door to at least one group. If the **Groups** list is empty, create a new group. See *Create and Edit Groups on page 27*.
4. Click **Add identification type** and select which credentials users need to present to the reader to be granted access to the door. See *Identification Types on page 28*.
Add at least one identification type to each door.
5. To add multiple identification types, repeat the previous step.


AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management


If both identification types **Card number only** and **PIN only** are added, users can choose to either swipe their card or enter their pin to access the door. But if, instead, only the identification type **Card number and PIN** is added, users must both swipe their card and enter their PIN to access the door.

6. To define when the credentials are valid, drag a schedule to each identification type.


To manually unlock doors, lock doors, or grant temporary access, click one of the manual door actions as required. See *Use Manual Door Actions on page 29*.

To expand an item in the Doors list, click .

To edit a door or reader name, click  and make the changes. Then click **Save**.

To verify the reader, identification type, and access schedule combinations, click .

To verify the function of the locks connected to the doors, click the verification controls. See *Verification Controls on page 17*.

To delete identification types or access schedules, click .

Identification Types

Identification types are portable credential storage devices, pieces of memorized information, or various combinations of the two that determine how users will be granted access to the door. Common identification types include tokens such as cards or key fobs, personal identification numbers (PINs), and request to exit (REX) devices.

For more information about credentials, see *User Credentials on page 30*.


The following identification types are available:

- **Card number only** – The user can access the door using only a card or other token accepted by the reader. The card number is a unique number that is usually printed on the card. See the card manufacturer's information about where to locate the card number. The card number can also be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**.
- **Card raw only** – The user can access the door using only a card or other token accepted by the reader. The information is stored as raw data on the card. The card raw data can be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**. Only use this identification type if a card number cannot be located.
- **PIN only** – The user can access the door using only a four-digit personal identification number (PIN).
- **Card number and PIN** – The user needs both the card, or other token accepted by the reader, and a PIN to access the door. The user must present the credentials in the specified order (card first, then PIN).
- **Card raw and PIN** – The user needs both the card, or other token accepted by the reader, and a PIN to access the door. Only use this identification type if a card number cannot be located. The user must present the credentials in the specified order (card first, then PIN).
- **REX** – The user can access the door by activating a request to exit (REX) device, such as a button, sensor, or push bar.

Add Scheduled Unlock States

To automatically keep a door unlocked for a specific duration of time, you can add a **Scheduled unlock** state to a door and apply an access schedule to it.


For example, to keep a door unlocked during office hours:

1. Go to **Access Management** and select the **Doors** tab.
2. Click  next to the **Doors** list item you want to edit.
3. Click **Add scheduled unlock**.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management

4. Select the **Unlock** state (unlocked or unlock both locks depending on whether the door has one or two locks).
5. Click **OK**.
6. Apply the predefined **Office hours** access schedule to the **Scheduled unlock** state.


To verify when the door is unlocked, click .

To delete a scheduled unlock state or access schedule, click .

Use Manual Door Actions

Doors can be unlocked or locked and temporary access can be granted in the **Doors** tab through the **Manual door actions**. Which manual door actions are available for a specific door depends on how the door has been configured.

To use the manual door actions:

1. Go to **Access Management** and select the **Doors** tab.
2. In the **Doors** list, click  next to the door that you want to control.
3. Click the required door action. See *Manual Door Actions on page 29*.

Note

To use the manual door actions, you need to open the Access Management page through the door controller the specific door is connected to. If you open the Access Management page through a different door controller, instead of the manual door actions there will be a link to the Overview page of the door controller the specific door is connected to. Click the link, go to **Access Management**, and select the **Doors** tab.

Manual Door Actions

The following manual door actions are available:

- **Get door status** – Verify the current state of the door monitor, door alarms, and locks.
- **Access** – Grant users access to the door. The given access time applies. See *Configure Locks and Door Monitors on page 14*.
- **Unlock (one lock)** or **Unlock both locks (two locks)** – Unlock the door. The door remains unlocked until you press **Lock** or **Lock both locks**, a scheduled door state is activated, or the door controller is restarted.
- **Lock (one lock)** or **Lock both locks (two locks)** – Lock the door.
- **Unlock second lock and lock primary** – This option is only available if the door has been configured with a secondary lock. Unlock the door. The secondary lock remains unlocked until you press **Double lock** or a scheduled door state is activated.

Create and Edit Users

Each person must have a unique user profile to be granted access to doors in the access control system. The user profile consists of credentials that tell the system who the user is and when and how they are granted access to the doors.

To be able to manage the user access rights efficiently, each user must belong to one or more groups. For more information, see *Create and Edit Groups*.


To create a new user profile:

1. Go to **Access Management**.
2. Select the **Users** tab and click **Add new user**.
3. In the **Add User** dialog, enter the user's credentials. See *User Credentials on page 30*.


AXIS A1001 Network Door Controller & AXIS Entry Manager


Access Management

4. Click **Save**.
5. Drag the user to one or more groups in the **Groups** list. If the **Groups** list is empty, create a new group. See *Create and Edit Groups on page 27*.

To expand an item in the **Users** list and view a user's credentials, click .

To find a specific user, enter a filter in the filter users field. To force exact matches, surround the filter text with double quotation marks, for example "John" or "potter, virginia".

To edit a user's credentials, click  and change the credentials as required. Then click **Save**.

To delete a user, click .

User Credentials

The following credentials are available for users:

- **First name** (required)
- **Last name**
- **Valid from** and **Valid until** – Enter the dates between which the user's credentials shall be valid. Click the date field and select the desired month, day, and year. You can also type the date directly in the field.
- **Suspend user** – Select to suspend the user. When suspended, the user cannot access any doors in the system. Deselect to give the user access again. Suspension is intended to be temporary. If the user shall be denied access permanently, it is better to delete the user profile.
- **PIN** (required if no card number or card raw) – Enter the four-digit personal identification number (PIN) selected by or assigned to the user.
- **Card number** (required if no PIN or card raw) – Enter the card number. See the card manufacturer's information about where to locate the card number. The card number can also be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**.
- **Card raw** (required if no PIN or card number) – Enter the card raw data. The data can be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**. Only use this identification type if a card number cannot be located.

Note

- To be able to save the profile, you must enter the user's **First name** or **Last name** and either the **PIN**, **Card number**, or **Card raw** data.
- The **Retrieve** button is only available if the hardware configuration has been completed and one or more readers are connected to the controller.

Import Users

Users can be added to the system by importing a text file in comma-separated value (CSV) format. It is recommended to import users when you need to add many users at a time.

Before you can import users, you must create and save a file (*.csv or *.txt) in the correct CSV format. Separate values by commas, no spaces, and separate each user with a line break.

Example

```
virginia,potter,1212,56781234
jane,doe,1234,12345678
leia,garfunkel,8545,45673258
ororo,wolf,3548,78542654
john,doe,5435,87654321
```

To import users:

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management

1. Go to **Setup > Import Users**.
2. Locate and select the *.csv or *.txt file that holds the list of users.
3. Select the correct credential option for each column.
4. To import the users to the system, click **Import users**.
5. Verify that each column contains the correct type of credential.
6. If the columns are correct, click **Start importing users**. If the columns are incorrect, click **Cancel** and start over.
7. When the import is finished, click **OK**.

The following credential options are available:

- **First name**
- **Last name**
- **PIN code**
- **Card number**
- **Unassigned** – Values that will not be imported. Select this option to skip a particular column.

For more information about credentials, see *Create and Edit Users*.

Export Users

The Export page shows a comma-separated value (CSV) list of all the users in the system. The list can be used to import the users to another system.

To export the user list:

1. Open a plain text editor and create a new document.
2. Go to **Setup > Export Users**
3. Select all the values on the page and copy them.
4. Paste the values into the text document.
5. Save the document as a comma-separated value file (*.csv) or as a text (*.txt) file.

Example Access Schedule Combinations

Identification type schedules and group schedules can be combined in several ways to achieve different results. The examples below follow the workflow described on *page 24*.

Example

To create a schedule combination that

- grants guards access to a door at all times,
 - using their card during day shift hours (Monday–Friday, 6 a.m. to 4 p.m.), while
 - using their card and PIN before and after day shift hours, and that
 - grants day shift personnel access to the same door,
 - using their card during day shift hours only:
1. Create an **Addition** schedule called **Day shift hours**. See *page 25*.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Access Management

2. Create a day shift hours **Schedule item** that recurs Monday–Friday, 06:00–16:00.
3. Create two groups, one **Group** called **Guards** and one **Group** called **Day shift personnel**. See *page 27*.
4. Drag the predefined **Always** access schedule to the **Guards** group.
5. Drag the **Day shift hours** access schedule to the **Day shift personnel** group.
6. Add the **Card number and PIN** and **Card number only** identification types to the door's reader.
7. Drag the predefined **Always** access schedule to the **Card number and PIN** identification type.
8. Drag the **Day shift hours** access schedule to the **Card number only** identification type.
9. Drag the door to both groups. Then add users to the groups as required. See *page 29*.

Example

To create a schedule combination that

- grants guards access to a door at all times,
 - using their card during day shift hours (Monday–Friday, 6 a.m. to 4 p.m.), while
 - using their card and PIN before and after day shift hours, and that
 - grants day shift personnel access to the same door every day between 6 a.m. and 4 p.m.,
 - using their card during day shift hours, while
 - using their card and PIN during nights and weekends:
1. Create an **Addition** schedule called **Day shift hours**. See *page 25*.
 2. Create a day shift hours **Schedule item** that recurs Monday–Friday, 06:00–16:00.
 3. Create a **Subtraction** schedule called **Nights & weekends**.
 4. Create a nights and weekends **Schedule item** that recurs Sunday–Saturday 16:00–06:00.
 5. Drag the predefined **Always** schedule and the **Nights & weekends** access schedule to the **Day shift personnel** group.
 6. Create two groups, one **Group** called **Guards** and one **Group** called **Day shift personnel**. See *page 27*.
 7. Drag the predefined **Always** access schedule to the **Guards** group and the **Day shift personnel** group.
 8. Drag the **Nights & weekends** access schedule to the **Day shift personnel** group.
 9. Add the **Card number and PIN** and **Card number only** identification types to the door's reader.
 10. Drag the predefined **Always** access schedule to the **Card number and PIN** identification type.
 11. Drag the **Day shift hours** access schedule to the **Card number only** identification type.
 12. Drag the door to both groups. Then add users to the groups as required. See *page 29*.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Alarm and Event Configuration

Alarm and Event Configuration


Events that occur in the system, for example when a user swipes a card or a REX device is activated, are logged in the event log. Logged events can be configured to trigger alarms and such alarms are logged in the alarm log.

- View the event log. See *page 33*.
- View the alarm log. See *page 33*.
- Configure the event and alarm logs. See *page 33*.

Alarms can also be configured to trigger actions such as email notifications. For more information, see *Set Up Action Rules on page 34*.

View the Event Log

To view logged events, go to **Event Log**. If global events is enabled, you can open the event log from any door controller in the system. For more information about global events, see *Configure the Event and Alarm Logs on page 33*.

To expand an item in the event log and view the event details, click .

Applying filters to the event log makes it easier to find specific events. To filter the list, select one or several event log filters and click **Refresh list**. For more information, see *Event Log Filters on page 33*.

As an administrator, you might have more interest in some events than others. Therefore, you can choose which events that shall be logged, and for which controllers. For more information, see *Event Log Options on page 34*.


Event Log Filters

You can narrow the scope of the event log by selecting one or several of the following filters:

- Topic – Select the event in the **Filter by topics** list.
- Door controller – Select the controller in the **Filter by controller** list.
- Date and time – under **Filter by date and time**, select **Based on date and time interval** and enter the desired time range.

View the Alarm Log

To view the triggered alarms, go to **Alarm Log**. If global events is enabled, you can open the alarm log from any door controller in the system. For more information about global events, see *Configure the Event and Alarm Logs on page 33*.

To expand an item in the alarm log and view the alarm details, for example door identity and state, click .

To remove an alarm from the list after verifying the cause of the alarm, click **Acknowledge**.

As an administrator, you might need some events to trigger alarms. Therefore, you can choose which events shall trigger alarms and for which controllers. For more information, see *Alarm Log Options*.

Configure the Event and Alarm Logs

The **Configure Event and Alarm Logs** page allows you to define which events shall be logged and trigger alarms.

To share events and alarms between all connected controllers, select **Global events**. When global events is enabled, you only need to open one **Event Log** page and one **Alarm Log** page to simultaneously manage the events and alarms of all door controllers in the system. Global events is enabled by default.

If you disable global events, you will have to open one **Event Log** page and one **Alarm Log** page for each individual door controller and manage their events and alarms separately.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Alarm and Event Configuration

Important

Each time that you enable or disable global events, the event log is cleared. This means that all events before that moment are removed and the event log starts over.

Alarms can also be configured to trigger actions such as email notifications. For more information, see *Set Up Action Rules on page 34*.

Event Log Options

To define which events shall be included in the event log, go to **Setup > Configure Event and Alarm Logs**.

The following options for logging events are available:

- **No logging** – Disable event logging. The event will not be registered or included in the event log.
- **Log for all controllers** – Enable event logging in all door controllers. The event will be registered for all controllers and included in the event log.
- **Log for selected controllers** – Enable event logging in selected door controllers. The event will be registered for all selected controllers and included in the event log. Select this option for events that will be combined with either the alarm log option **No alarms** or **Log alarm for selected controllers**.

In the **Configure event logging** list, click **Select controllers** under the event log item you want to enable. The **Device Specific Event Logging** dialog opens. Under **Log event**, select the controllers that shall have alarm logging enabled and click **Save**.

Alarm Log Options

To define which events should trigger an alarm, go to **Setup > Configure Event and Alarm Logs**.

The following options for triggering and logging alarms are available:

- **No alarms** – Disable alarm logging. The event will not trigger any alarms or be included in the alarm log.
- **Log alarm for all controllers** – Enable alarm logging in all door controllers. The event will trigger an alarm and be included in the alarm log.
- **Log alarm for selected controllers** – Enable alarm logging in selected door controllers. The event will trigger an alarm and be included in the alarm log.

In the **Configure alarm logging** list, click **Select controllers** under the alarm log item you want to enable. The **Device Specific Alarm Triggering** dialog opens. Under **Trigger alarm**, select the door controllers that shall have alarm logging enabled and click **Save**.

Set Up Action Rules

The Event pages allow you to configure the Axis product to perform actions when different events occur. For example, the product can send an email notification or activate an output port when an alarm is triggered. The set of conditions that defines how and when the action is triggered is called an action rule. If multiple conditions are defined, all of them must be met to trigger the action.

For more information about available triggers and actions, see *Triggers on page 35* and *Actions on page 37*.

The following example describes how to set up an action rule to send an email notification when any alarm is triggered.

1. Configure the alarms. See *Configure the Event and Alarm Logs on page 33*.
2. Go to **Setup > Additional Controller Configuration > Events > Action Rules** and click **Add**.
3. Select **Enable rule** and enter a descriptive name for the rule.
4. Select **Event Logger** from the **Trigger** drop-down list.
5. Optionally, select a **Schedule** and **Additional conditions**. See below.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Alarm and Event Configuration


6. Under **Actions**, select **Send Notification** from the **Type** drop-down list.
7. Select an email recipient from the drop-down list. See *Add Recipients on page 37*.

The following example describes how to set up an action rule to activate an output port when the door is forced open.

1. Go to **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports**.
2. Select **Output** from the desired **I/O Port Type** drop-down list and enter a **Name**.
3. Select the I/O port's **Normal state** and click **Save**.
4. Go to **Events > Action Rules** and click **Add**.
5. Select **Door** from the **Trigger** drop-down list.
6. Select **Door Alarm** from the drop-down list.
7. Select the desired door from the drop-down list.
8. Select **DoorForcedOpen** from the drop-down list.
9. Optionally, select a **Schedule** and **Additional conditions**. See below.
10. Under **Actions**, select **Output Port** from the **Type** drop-down list.
11. Select the desired output port from the **Port** drop-down list.
12. Set state **Active**.
13. Select **Duration** and **Go to opposite state after**. Then enter the desired duration of the action.
14. Click **OK**.

To use more than one trigger for the action rule, select **Additional conditions** and click **Add** to add additional triggers. When using additional conditions, all conditions must be met to trigger the action.

To prevent an action from being triggered repeatedly, a **Wait at least time** can be set. Enter the time in hours, minutes and seconds, during which the trigger should be ignored before the action rule can be activated again.

For more information, see the online help .

Triggers

Available action rule **triggers** and **conditions** include:

- **Access Point**
 - **Access Point Enabled** – Triggers the action rule when an access point device such as a reader or REX device is configured, for example when the hardware configuration is completed or an identification type is added.
- **Configuration**
 - **Access Point Changed** – Triggers the action rule when the configuration of an access point device such as a reader or REX device is changed, for example when hardware is configured or an identification type is edited, changing the ways through which a door can be accessed.
 - **Access Point Removed** – Triggers the action rule when the hardware configuration of an access point device such as a reader or REX device is reset.
 - **Area Changed** – Not supported by this version of AXIS Entry Manager. Must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use devices that can provide the required signals. Triggers the action rule when an access area is changed.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Alarm and Event Configuration

- **Area Removed** – Not supported by this version of AXIS Entry Manager. Must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use devices that can provide the required signals. Triggers the action rule when an access area is removed from the system.
- **Door Changed** – Triggers the action rule when the door configuration settings, for example door name, are changed or when a door is added to the system. This can for example be used to send a notification when a door is installed and configured.
- **Door Removed** – Triggers the action rule when a door is removed from the system. This can for example be used to send a notification when a door is removed from the system.
- **Door**
 - **Door Alarm** – Triggers the action rule when the door monitor indicates that the door has been forced open, the door is open too long, or if the door is faulty in any way. This can for example be used to send a notification when someone is forcing an entry.
 - **Door Double-Lock Monitor** – Triggers the action rule only when the secondary lock changes state to either locked or unlocked.
 - **Door Lock Monitor** – Triggers the action rule when the normal lock changes state to either locked or unlocked. For example, a fault is triggered when the door monitor detects that the door is open although the lock is locked.
 - **Door Mode** – Triggers the action rule when the door changes states, for example, when the door has been accessed or blocked, or the door is in lockdown mode. For more detailed descriptions of these modes, see the online help.
 - **Door Monitor** – Triggers the action rule when the door monitor state changes. This can for example be used to send a notification when a door monitor indicates that the door is opened or closed.
 - **Door Tamper** – Triggers the action rule when the door monitor detects that the connection is interrupted, for example if someone cuts the wires to the door monitor. To use this trigger, make sure that **Enable supervised inputs** is selected and that end of line resistors are installed on the relevant door connector input ports. For more information, see *Use Supervised Inputs on page 16*.
 - **Door Warning** – Triggers the action rule before the door open too long alarm goes off. This can be used to, for example, send a warning signal that the door controller will send the real alarm, the door open too long alarm, if the door is not closed within the specified door open too long time. For more information about door open too long time, see *Configure Locks and Door Monitors on page 14*.
- **Event Logger** – Keeps track of all events in the door controller, for example when a user swipes a card or opens a door. If **Global events** is enabled, the event logger keeps track of all the events in every controller in the system. To set which alarms and events that can trigger an action rule, go to **Setup > Configure Event and Alarm Logs**. The event logger is shared by the system and can store up to 30 000 events. When the limit is reached, the event logger uses the first in first out (FIFO) rule. This means that the first event is the first to be overwritten.
 - **Alarm** – Triggers the action rule when one of the specified alarms has been triggered. The system administrator can configure which events are more important than others and select whether a particular event should trigger an alarm or not.
 - **Dropped Alarms** – Triggers the action rule when new alarm records cannot be written to the alarm logs. For example if there are so many simultaneous alarms that the event logger cannot keep up. When an alarm is dropped, a notification can be sent to the operator.
 - **Dropped Events** – Triggers the action rule when new event records cannot be written to the event logs. For example, if there are so many simultaneous events that the event logger cannot keep up. When an event is dropped, a notification can be sent to the operator.
- **Hardware**
 - **Casing Open** – Triggers the action rule if the cover of the door controller is opened or if the door controller is removed from the wall or ceiling. This can for example be used to send a notification if the casing has been opened for maintenance purposes or when someone has tampered with the casing.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Alarm and Event Configuration

- **Network** – Triggers the action rule when the network connection is lost. Select **Yes** to trigger the action rule when the network connection is lost. Select **No** to trigger the action rule when the network connection is restored.
- **Peer Connection** – Triggers the action rule when the Axis product has established a connection with another door controller, if the network connection between the devices is lost, or if the pairing of door controllers has failed. This can for example be used to send a notification that a door controller has lost its network connection.
- **Input Signal**
 - **Digital Input Port** – Trigger the rule when an I/O port receives a signal from a connected device. See *I/O Ports on page 48*.
 - **Manual Trigger** – Triggers the action rule when the manual trigger is activated. It can be used by a client such as an access management system, through the VAPIX® application programming interface, to manually start or stop the action rule.
 - **Virtual Inputs** – Triggers the action rule when one of the virtual inputs changes states. It can be used by a client such as an access management system, through the VAPIX® application programming interface, to trigger actions. Virtual inputs can, for example, be connected to buttons in the management system's user interface.
- **Schedule**
 - **Interval** – Triggers the action rule at the schedule's start time and remains active until the schedule's end time is reached.
 - **Pulse** – Triggers the action rule when a one-time event occurs. That is, an event that happens at a specific time and has no duration.
- **System**
 - **System Ready** – Triggers the action rule when the system is in state ready. For example, the Axis product can detect the system state and send a notification when the system has started.

Select **Yes** to trigger the action rule when the product is in state ready. Note that the rule will only trigger when all necessary services, such as the event system, has started.
- **Time**
 - **Recurrence** – Triggers the action rule by monitoring the recurrences that you have created. You can use this trigger to initiate recurring actions such as sending notifications every hour. Select a recurrence pattern or create a new one. For more information about setting up a recurrence pattern, see *Set Up Recurrences on page 39*.
 - **Use Schedule** – Trigger the rule according to the selected schedule. See *Create Schedules on page 38*.

Actions

Available actions include:

- **Output Port** – Activate an I/O port to control an external device.
- **Send Notifications** – Send a notification message to a recipient.
- **Status LED** – The status LED can be set to flash for the duration of the action rule or for a set number of seconds. The status LED can be used during installation and configuration to visually validate if the trigger settings, for example the door open too long trigger, work correctly. To set the status LED flash color, select an **LED Color** from the drop-down list.

Add Recipients

The product can send messages to notify administrators about events and alarms. But before the product can send notification messages, you must define one or more recipients. For information about available options, see *Recipient Types on page 38*.

To add a recipient:

AXIS A1001 Network Door Controller & AXIS Entry Manager

Alarm and Event Configuration

1. Go to **Setup > Additional Controller Configuration > Events > Recipients** and click **Add**.
2. Enter a descriptive name.
3. Select a recipient **Type**.
4. Enter the information needed for the recipient type.
5. Click **Test** to test the connection to the recipient.
6. Click **OK**.

Recipient Types

The following recipients are available:

- HTTP
- HTTPS
- Email
- TCP

Set Up Email Recipients

Email recipients can be configured by selecting one of the listed email providers, or by specifying the SMTP server, port and authentication used by, for example, a corporate email server.

Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid delivery problems and locked email accounts.

To set up an email recipient using one of the listed providers:

1. Go to **Events > Recipients** and click **Add**.
2. Enter a **Name** and select **Email** from the **Type** list.
3. Enter the email addresses to send emails to in the **To** field. Use commas to separate multiple addresses.
4. Select the email provider from the **Provider** list.
5. Enter the user ID and password for the email account.
6. Click **Test** to send a test email.

To set up an email recipient using for example a corporate email server, follow the instructions above but select **User defined as Provider**. Enter the email address to appear as sender in the **From** field. Select **Advanced settings** and specify the SMTP server address, port and authentication method. Optionally, select **Use encryption** to send emails over an encrypted connection. The server certificate can be validated using the certificates available in the Axis product. For information on how to upload certificates, see *Certificates on page 42*.

Create Schedules

Schedules can be used as action rule triggers or as additional conditions. Use one of the predefined schedules or create a new schedule as described below.

To create a new schedule:

1. Go to **Setup > Additional Controller Configuration > Events > Schedules** and click **Add**.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Alarm and Event Configuration

2. Enter a descriptive name and the information needed for a daily, weekly, monthly or yearly schedule.
3. Click **OK**.

To use the schedule in an action rule, select the schedule from the **Schedule** drop-down list in the **Action Rule Setup** page.

Set Up Recurrences

Recurrences are used to trigger action rules repeatedly, for example every 5 minutes or every hour.

To set up a recurrence:

1. Go to **Setup > Additional Controller Configuration > Events > Recurrences** and click **Add**.
2. Enter a descriptive name and recurrence pattern.
3. Click **OK**.

To use the recurrence in an action rule, first select **Time** from the **Trigger** drop-down list in the **Action Rule Setup** page and then select the recurrence from the second drop-down list.

To modify or remove recurrences, select the recurrence in the **Recurrences List** and click **Modify** or **Remove**.

Reader Feedback

Readers use LEDs and beepers to send feedback messages to the user (the person accessing or trying to access the door). The door controller can trigger a number of feedback messages, some of which are preconfigured in the door controller and supported by most readers.

Readers have different LED behaviors, but typically they use different sequences of steady lights and flashing lights in red, green, and amber.

Readers can also use one-pitch beepers to send messages, using different sequences of short and long beeper signals.

The table below shows the events that are preconfigured in the door controller to trigger reader feedback and their typical reader feedback signals.

Event	Wiegand dual LED	Wiegand single LED	OSDP	Beeper pattern	State
Idle	Off	Red	Red	Silent	Normal
RequirePIN	Flashing red/green	Flashing red/green	Flashing red/green	Two short beeps	PIN required
AccessGranted	Green	Green	Green	One short beep	Access granted
AccessDenied	Red	Red	Red	One long beep	Access denied

Feedback messages other than the above must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use readers that can provide the required signals. For more information, see the user information supplied by the access management system developer and reader manufacturer.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Reports

Reports

The Reports page allows you to view, print, and export reports that contain different types of information about the system. For more information about which reports that are available, see *Report Types on page 40*.

View, Print, and Export Reports


To open the Reports page, click **Reports**.

To view a report, click **View and print**.

To print a report:

1. Click **View and print**.
2. Select the columns that shall be included in the report. All columns are selected by default.
3. If you want to narrow the scope of the report, enter a filter in the relevant filter field. For example, you can filter users by which group they belong to, doors by their schedules, or groups by the doors they have access to.

To force exact matches, surround the filter text with double quotation marks, for example "John".

4. If you want to sort the report items in a different order, click  in the relevant column. To change between standard and reverse order, toggle the sorting buttons.

▲ Shows the items in standard order (ascending).

▼ Shows the items in reverse order (descending).

5. Click **Print selected columns**.

To export a report, click **Export CSV file**.

The report will be exported as a comma-separated value (CSV) file and will include all possible columns and items for the report type. Unless otherwise specified, the exported file (*.csv) is saved in the default download folder. You can select a download folder in the web browser's user settings.

Report Types

The following report types are available:

- Access schedules. For more information about access schedule types and options, see *page 25* and *page 26*.
- Groups. For more information about group credentials, see *page 27*.
- Doors. For more information about doors and identification types, see *page 27* and *page 28*.
- Users. For more information about user credentials, see *page 30*.
- Door controllers. For more information about connected controllers and their ID types, see *page 21*. For more information about door monitor time options, see *page 15*.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

System Options

Security

Users

User access control is enabled by default and can be configured under **Setup > Additional Controller Configuration > System Options > Security > Users**. An administrator can set up other users by giving them user names and passwords.

The user list displays authorized users and user groups (access levels):

Administrator – Unrestricted access to all settings; can add, modify and remove other users.

Under **HTTP/RTSP Password Settings**, select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you upgraded the firmware and existing clients support encryption but need to log in again and be configured to use this functionality.

Deselect the **Enable Basic Setup** option to hide the Basic Setup menu. Basic Setup provides quick access to settings that should be made before using the Axis product.

ONVIF

ONVIF (Open Network Video Interface Forum) is a global interface standard that makes it easier for end users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost and future-proof systems.

By creating a user you automatically enable ONVIF communication. Use the user name and password with all ONVIF communication with the product. For more information see www.onvif.org

IP Address Filter

IP address filtering is enabled on the **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter** page. Once enabled, the listed IP address are allowed or denied access to the Axis product. Select **Allow** or **Deny** from the list and click **Apply** to enable IP address filtering.

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol providing encrypted browsing. HTTPS can also be used by users and clients to verify that the correct device is being accessed. The security level provided by HTTPS is considered adequate for most commercial exchanges.

The Axis product can be configured to require HTTPS when administrators log in.

To use HTTPS, an HTTPS certificate must first be installed. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates** to install and manage certificates. See *Certificates on page 42*.

To enable HTTPS on the Axis product:

1. Go to **Setup > Additional Controller Configuration > System Options > Security > HTTPS**
2. Select an HTTPS certificate from the list of installed certificates.
3. Optionally, click **Ciphers** and select the encryption algorithms to use for SSL.
4. Set the **HTTPS Connection Policy** for the different user groups.
5. Click **Save** to enable the settings.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

To access the Axis product via the desired protocol, enter `https://` or `http://` in the address field in a browser.

The HTTPS port can be changed on the **System Options > Network > TCP/IP > Advanced** page.

IEEE 802.1X

IEEE 802.1X is a standard for port-based Network Admission Control providing secure authentication of wired and wireless network devices. IEEE 802.1X is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1X, devices must be authenticated. The authentication is performed by an authentication server, typically a **RADIUS** server, examples of which are FreeRADIUS and Microsoft Internet Authentication Service.

In Axis implementation, the Axis product and the authentication server identify themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by a **Certification Authority (CA)**. You need:

- a CA certificate to authenticate the authentication server.
- a CA-signed client certificate to authenticate the Axis product.

To create and install certificates, go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**. See *Certificates on page 42*. Many CA certificates are preinstalled.

To allow the product to access a network protected by IEEE 802.1X:

1. Go to **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X**.
2. Select a **CA Certificate** and a **Client Certificate** from the lists of installed certificates.
3. Under **Settings**, select the EAPOL version and provide the EAP identity associated with the client certificate.
4. Check the box to enable IEEE 802.1X and click **Save**.

Note

For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time on page 43*.

Certificates

Certificates are used to authenticate devices on a network. Typical applications include encrypted web browsing (HTTPS), network protection via IEEE 802.1X and secure upload of images and notification messages for example via email. Two types of certificates can be used with the Axis product:

Server/Client certificates – To authenticate the Axis product.

CA certificates – To authenticate peer certificates, for example the certificate of an authentication server in case the Axis product is connected to an IEEE 802.1X protected network.

Note

Installed certificates, except preinstalled CA certificates, will be deleted if the product is reset to factory default. Preinstalled CA certificates that have been deleted will be reinstalled.

A **Server/Client** certificate can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.

To install a self-signed certificate:

1. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**.
2. Click **Create self-signed certificate** and provide the requested information.

To create and install a CA-signed certificate:

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

1. Create a self-signed certificate as described above.
2. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**.
3. Click **Create certificate signing request** and provide the requested information.
4. Copy the PEM-formatted request and send to the CA of your choice.
5. When the signed certificate is returned, click **Install certificate** and upload the certificate.

Server/Client certificates can be installed as **Certificate from signing request** or as **Certificate and private key**. Select **Certificate and private key** if the private key is to be upload as a separate file or if the certificate is in PKCS#12 format.

The Axis product is shipped with several preinstalled CA certificates. If required, additional CA certificates can be installed:

1. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**.
2. Click **Install certificate** and upload the certificate.

Date & Time

The Axis product's date and time settings are configured under **Setup > Additional Controller Configuration > System Options > Date & Time**.

Current Server Time displays the current date and time (24h clock).

To change the date and time settings, select the preferred **Time mode** under **New Server Time**:

- **Synchronize with computer time** – Sets date and time according to the computer's clock. With this option, date and time are set once and will not be updated automatically.
- **Synchronize with NTP Server** – Obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see *NTP Configuration on page 45*.

If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 45*.
- **Set manually** – Allows you to manually set date and time.

If using an NTP server, select your **Time zone** from the drop-down list. If required, check **Automatically adjust for daylight saving time changes**.

Network

Basic TCP/IP Settings

The Axis product supports IP version 4 (IPv4).

The Axis product can get an IPv4 address in the following ways:

- **Dynamic IP address – Obtain IP address via DHCP** is selected by default. This means that the Axis product is set to get the IP address automatically via Dynamic Host Configuration Protocol (DHCP).

DHCP allows network administrators to centrally manage and automate the assignment of IP addresses.
- **Static IP address** – To use a static IP address, select **Use the following IP address** and specify the IP address, subnet mask and default router. Then click **Save**.

DHCP should only be enabled when using dynamic IP address notification, or if the DHCP can update a DNS server that makes it possible to access the Axis product by name (host name).

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

If DHCP is enabled and the product cannot be accessed, run AXIS IP Utility to search the network for connected Axis products, or reset the product to the factory default settings and then perform the installation again. For information about how to reset to factory default, see *page 50*.

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign IP Address Using ARP/Ping on page 44*.

The ARP/Ping service is enabled by default but is automatically disabled two minutes after the product is started, or as soon as an IP address is assigned. To re-assign IP address using ARP/Ping, the product must be restarted to enable ARP/Ping for an additional two minutes.

To disable the service, go to **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic** and clear the option **Enable ARP/Ping setting of IP address**.

Pinging the product is still possible when the service is disabled.

Assign IP Address Using ARP/Ping

The product's IP address can be assigned using ARP/Ping. The command must be issued within 2 minutes of connecting power.

1. Acquire a free static IP address on the same network segment as the computer.
2. Locate the serial number (S/N) on the product label.
3. Open a command prompt and enter the following commands:

Linux/Unix syntax

```
arp -s <IP address> <serial number> temp  
ping -s 408 <IP address>
```

Linux/Unix example

```
arp -s 192.168.0.125 00:40:8c:18:10:00 temp  
ping -s 408 192.168.0.125
```

Windows syntax (this may require that you run the command prompt as an administrator)

```
arp -s <IP address> <serial number>  
ping -l 408 -t <IP address>
```

Windows example (this may require that you run the command prompt as an administrator)

```
arp -s 192.168.0.125 00-40-8c-18-10-00  
ping -l 408 -t 192.168.0.125
```

4. Check that the network cable is connected and then restart the product by disconnecting and reconnecting power.
5. Close the command prompt when the product responds with `Reply from 192.168.0.125: . . .` or similar.
6. Open a browser and type `http://<IP address>` in the Location/Address field.

For other methods of assigning the IP address, you may find the document *Assign an IP Address and Access the Video Stream* on Axis Support web at www.axis.com/techsup useful.

Note

- To open a command prompt in Windows, open the **Start menu** and type `cmd` in the **Run/Search** field.
- To use the ARP command in Windows 8/Windows 7/Windows Vista, right-click the command prompt icon and select **Run as administrator**.
- To open a command prompt in Mac OS X, open the Terminal utility from **Application > Utilities**.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

AXIS Video Hosting System (AVHS)

AVHS used in conjunction with an AVHS service, provides easy and secure Internet access to controller management and logs accessible from any location. For more information and help to find a local AVHS Service Provider go to www.axis.com/hosting

The AVHS settings are configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic**. The possibility to connect to an AVHS service is enabled by default. To disable, clear the **Enable AVHS** box.

One-click enabled – Press and hold the product's control button (see *Hardware Overview on page 5*) for about 3 seconds to connect to an AVHS service over the Internet. Once registered, **Always** will be enabled and the Axis product stays connected to the AVHS service. If the product is not registered within 24 hours from when the button is pressed, the product will disconnect from the AVHS service.

Always – The Axis product will constantly attempt to connect to the AVHS service over the Internet. Once registered the product will stay connected to the service. This option can be used when the product is already installed and it is not convenient to use the one-click installation.

Note

AVHS support is dependent on the availability of subscriptions from service providers.

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service assigns a host name for easy access to the product. For more information, see www.axiscam.net

To register the Axis product with AXIS Internet Dynamic DNS Service, go to **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic**. Under **Services**, click the **AXIS Internet Dynamic DNS Service Settings** button (requires access to the Internet). The domain name currently registered at AXIS Internet Dynamic DNS service for the product can at any time be removed.

Note

AXIS Internet Dynamic DNS Service requires IPv4.

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses. The DNS settings are configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

Select **Obtain DNS server address via DHCP** to use the DNS settings provided by the DHCP server.

To make manual settings, select **Use the following DNS server address** and specify the following:

Domain name – Enter the domain(s) to search for the host name used by the Axis product. Multiple domains can be separated by semicolons. The host name is always the first part of a fully qualified domain name, for example, `myserver` is the host name in the fully qualified domain name `myserver.mycompany.com` where `mycompany.com` is the domain name.

Primary/Secondary DNS server – Enter the IP addresses of the primary and secondary DNS servers. The secondary DNS server is optional and will be used if the primary is unavailable.

NTP Configuration

NTP (Network Time Protocol) is used to synchronize the clock times of devices in a network. The NTP settings are configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

Select **Obtain NTP server address via DHCP** to use the NTP settings provided by the DHCP server.

To make manual settings, select **Use the following NTP server address** and enter the host name or IP address of the NTP server.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options


Host Name Configuration

The Axis product can be accessed using a host name instead of an IP address. The host name is usually the same as the assigned DNS name. The host name is configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

Select **Obtain host name via IPv4 DHCP** to use host name provided by the DHCP server running on IPv4.

Select **Use the host name** to set the host name manually.

Select **Enable dynamic DNS updates** to dynamically update local DNS servers whenever the Axis product's IP address changes.

For more information, see the online help .

Link-Local IPv4 Address

Link-Local Address is enabled by default and assigns the Axis product an additional IP address which can be used to access the product from other hosts on the same segment on the local network. The product can have a Link-Local IP and a static or DHCP-supplied IP address at the same time.

This function can be disabled under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

HTTP

The HTTP port used by the Axis product can be changed under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 80, any port in the range 1024–65535 can be used.

HTTPS

The HTTPS port used by the Axis product can be changed under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 443, any port in the range 1024–65535 can be used.

To enable HTTPS, go to **Setup > Additional Controller Configuration > System Options > Security > HTTPS**. For more information, see *HTTPS* on page 41.

NAT traversal (port mapping) for IPv4

A network router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most routers are pre-configured to stop attempts to access the private network (LAN) from the public network (Internet).

Use **NAT traversal** when the Axis product is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the product.

NAT traversal is configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

Note

- For NAT traversal to work, this must be supported by the router. The router must also support UPnP™.
- In this context, router refers to any network routing device such as a NAT router, Network router, Internet Gateway, Broadband router, Broadband sharing device, or a software such as a firewall.

Enable/Disable – When enabled, the Axis product attempts to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the product (see **Setup > Additional Controller Configuration > System Options > Network > UPnP**).

Use manually selected NAT router – Select this option to manually select a NAT router and enter the IP address for the router in the field. If no router is specified, the product automatically searches for NAT routers on your network. If more than one router is found, the default router is selected.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

Alternative HTTP port – Select this option to manually define an external HTTP port. Enter a port in the range 1024–65535. If the port field is empty or contains the default setting, which is 0, a port number is automatically selected when enabling NAT traversal.

Note

- An alternative HTTP port can be used or be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this, enter a new port number and click **Save**.

FTP

The FTP server running in the Axis product enables upload of new firmware, user applications, etc. The FTP server can be disabled under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

RTSP


The RTSP server running in the Axis product allows a connecting client to start an event stream. The RTSP port number can be changed under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**. The default port is 554.

Note

Event streams will not be available if the RTSP server is disabled.

SOCKS

SOCKS is a networking proxy protocol. The Axis product can be configured to use a SOCKS server to reach networks on the other side of a firewall or proxy server. This functionality is useful if the Axis product is located on a local network behind a firewall, and notifications, uploads, alarms, etc need to be sent to a destination outside the local network (for example the Internet).

SOCKS is configured under **Setup > Additional Controller Configuration > System Options > Network > SOCKS**. For more information, see the online help .

QoS (Quality of Service)

QoS (Quality of Service) guarantees a certain level of a specified resource to selected traffic on a network. A QoS-aware network prioritizes network traffic and provides a greater network reliability by controlling the amount of bandwidth an application may use.

The QoS settings are configured under **Setup > Additional Controller Configuration > System Options > Network > QoS**. Using DSCP (Differentiated Services Codepoint) values, the Axis product can mark event/alarm traffic and management traffic.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

To enable and configure SNMP in the Axis product, go to the **Setup > Additional Controller Configuration > System Options > Network > SNMP** page.

Depending on the level of security required, select the version on SNMP to use.

Traps are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

Note

If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

Traps for SNMP v1/v2 are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

The following traps are available:

- Cold start
- Warm start
- Link up
- Authentication failed

SNMP v3 provides encryption and secure passwords. To use traps with SNMP v3, an SNMP v3 management application is required.

To use SNMP v3, HTTPS must be enabled, see *HTTPS on page 41*. To enable SNMP v3, check the box and provide the initial user password.

Note

The initial password can only be set once. If the password is lost, the Axis product must be reset to factory default, see *Reset to Factory Default Settings on page 50*.

UPnP™

The Axis product includes support for UPnP™. UPnP™ is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

UPnP™ can be disabled under **Setup > Additional Controller Configuration > System Options > Network > UPnP™**.

Bonjour

The Axis product includes support for Bonjour. Bonjour is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

Bonjour can be disabled under **Setup > Additional Controller Configuration > System Options > Network > Bonjour**.

Ports & Devices

I/O Ports

The auxiliary connector on the Axis product provides two configurable input and output ports for connection of external devices. For information about how to connect external devices, see the Installation Guide, available on www.axis.com

The I/O ports are configured under **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports**. Select the port direction (**Input** or **Output**). The ports can be given descriptive names and their **Normal states** can be configured as **Open circuit** or **Grounded circuit**.

Port Status

The list on the **System Options > Ports & Devices > Port Status** page shows the status of the product's input and output ports.

Maintenance

The Axis product provides several maintenance functions. These are available under **Setup > Additional Controller Configuration > System Options > Maintenance**.

Click **Restart** to perform a correct restart if the Axis product is not behaving as expected. This will not affect any of the current settings.

Note

A restart clears all entries in the Server Report.

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

Click **Restore** to reset most settings to the factory default values. The following settings are not affected:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the system time
- the IEEE 802.1X settings

Click **Default** to reset all settings, including the IP address, to the factory default values. This button should be used with caution. The Axis product can also be reset to factory default using the control button, see *Reset to Factory Default Settings on page 50*.

For information about firmware upgrade, see *Upgrade the Firmware on page 51*.

Support

Support Overview

The **Setup > Additional Controller Configuration > System Options > Support > Support Overview** page provides information on troubleshooting and contact information, should you require technical assistance.

See also *Troubleshooting on page 51*.

System Overview

To get an overview of the Axis product's status and settings, go to **Setup > Additional Controller Configuration > System Options > Support > System Overview**. Information that can be found here includes firmware version, IP address, network and security settings, event settings, and recent log items. Many of the captions are links to the proper Setup page.

Logs & Reports

The **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports** page generates logs and reports useful for system analysis and troubleshooting. If contacting Axis Support, please provide a valid Server Report with your query.

System Log – Provides information about system events.

Access Log – Lists all failed attempts to access the product. The Access Log can also be configured to list all connections to the product (see below).

Server Report – Provides information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.

Parameter List – Shows the product's parameters and their current settings. This may prove useful when troubleshooting or when contacting Axis Support.

Connection List – Lists all clients that are currently accessing media streams.

Crash Report – Generates an archive with debugging information. The report takes several minutes to generate.

The log levels for the System Log and the Access Log are set under **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration**. The Access Log can be configured to list all connections to the product (select Critical, Warnings & Info).

AXIS A1001 Network Door Controller & AXIS Entry Manager

System Options

Advanced

Scripting

Scripting allows experienced users to customize and use their own scripts.

NOTICE

Improper use may cause unexpected behavior and loss of contact with the Axis product.

Axis strongly recommends that you do not use this function unless you understand the consequences. Axis Support does not provide assistance for problems with customized scripts.

To open the Script Editor, go to **Setup > Additional Controller Configuration > System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 50*.

For more information, see www.axis.com/developer

File Upload

Files, for example webpages and images, can be uploaded to the Axis product and used as custom settings. To upload a file, go to **Setup > Additional Controller Configuration > System Options > Advanced > File Upload**.

Uploaded files are accessed through `http://<ip address>/local/<user>/<file name>` where <user> is the selected user group (viewer, operator or administrator) for the uploaded file.

Reset to Factory Default Settings

Important

Reset to factory default should be used with caution. A reset to factory default will reset all settings, including the IP address, to the factory default values.

Note

The installation and management software tools are available from the support pages on www.axis.com/techsup

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button and reconnect power. See *Hardware Overview on page 5*.
3. Keep the control button pressed for about 25 seconds until the status LED indicator turns amber for the second time.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90
5. Using the installation and management software tools, assign an IP address, set the password, and access the product.

It is also possible to reset parameters to factory default via the web interface. Go to **Setup > Additional Controller Configuration > Setup > System Options > Maintenance**.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Troubleshooting

Troubleshooting

Check the Firmware

Firmware is software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in the Axis product is displayed in the page **Setup > Additional Controller Configuration > Basic Setup** and in **Setup > Additional Controller Configuration > About**.

Upgrade the Firmware

Important

- Your dealer reserves the right to charge for any repair attributable to faulty upgrade by the user.
- Preconfigured and customized settings are saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

Note

- After the upgrade process has completed, the product will restart automatically. If restarting the product manually after the upgrade, always wait 5 minutes even if you suspect the upgrade has failed.
- Because the database of users, groups, credentials, and other data will be updating after a firmware upgrade, the first start-up could take a few minutes to complete. The time required is dependent on the amount of data.
- When you upgrade the Axis product with the latest firmware from Axis website, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before upgrading the firmware.

To upgrade the product's firmware:

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from Axis website at www.axis.com/techsup
2. Go to **Setup > Additional Controller Configuration > System Options > Maintenance** in the product's webpages.
3. Under **Upgrade Server**, click **Browse** and locate the file on your computer. Click **Upgrade**.
4. Wait approximately 5 minutes while the product is being upgraded and restarted. Then clear the web browser's cache.
5. Access the product.

Emergency Recovery Procedure

If power or network connection is lost during the upgrade, the process fails and the product becomes unresponsive. Flashing red Status indicator indicates a failed upgrade. To recover the product, follow the steps below. The serial number is found on the product's label.

1. In **UNIX/Linux**, type the following from the command line:

```
arp -s <IP address> <serial number> temp  
ping -l 408 <IP address>
```

In **Windows**, type the following from a command/DOS prompt (this may require that you run the command prompt as an administrator):

```
arp -s <IP address> <serial number>  
ping -l 408 -t <IP address>
```

2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press **CTRL+C** to stop Ping.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Troubleshooting

3. Open a browser and type in the product's IP address. In the page that opens, use the Browse button to select the upgrade file to use. Then click Load to restart the upgrade process.
4. After the upgrade is complete (1–10 minutes), the product automatically restarts and shows a steady green on the Status indicator.
5. Reinstall the product, referring to the Installation Guide.

If the emergency recovery procedure does not get the product up and running again, contact Axis support at www.axis.com/techsup/

Symptoms, Possible Causes and Remedial Actions

Problems setting the IP address

When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the product. Ensure the Ping length is set to 408. For instructions, see Installation Guide on www.axis.com .
The product is located on a different subnet	If the IP address intended for the product and the IP address of the computer used to access the product are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an IP address.
The IP address is being used by another device	Disconnect the Axis product from the network. Run the Ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the product): <ul style="list-style-type: none">• If you receive: <code>Reply from <IP address>: bytes=32; time=10...</code> this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the product.• If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.
Possible IP address conflict with another device on the same subnet.	The static IP address in the Axis product is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the product.

The product cannot be accessed from a browser

Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type <code>http</code> or <code>https</code> in the browser's address field. If the password for the user root is lost, the product must be reset to the factory default settings. See <i>Reset to Factory Default Settings on page 50</i> .
The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility to locate the product on the network. Identify the product using its model or serial number, or by the DNS name (if the name has been configured). If required, a static IP address can be assigned manually. For instructions, see Installation Guide on www.axis.com/techsup .
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See <i>Date & Time on page 43</i> .

The product is accessible locally but not externally

Router configuration	To configure your router to allow incoming data traffic to the Axis product, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the Axis product, see <i>NAT traversal (port mapping) for IPv4 on page 46</i> . The router must support UPnP™.
Firewall protection	Check the Internet firewall with your network administrator.
Default routers required	Check if you need to configure the router settings from Setup > Network Settings or Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic .

AXIS A1001 Network Door Controller & AXIS Entry Manager

Troubleshooting

Status and Network indicator LEDs are flashing red rapidly

Hardware failure

Contact your Axis reseller.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Technical Specifications

AXIS A1001 Network Door Controller

Function/group	Item	Specifications
	Models	AXIS A1001 Network Door Controller
Door controller	Readers	Up to 2 readers per controller (Wiegand, RS485 (OSDP) with supported card formats
	Doors	1–2 doors per controller ¹
	Credentials	Up to 15 000 with third-party access management software depending on server capacity
	Event history	30 000 First in First out (FIFO) per controller
	Access schedules	Unlimited or third-party software dependent
Digital I/O	I/O interface	<p>Reader I/O: DC output: 2x 12 V DC output max 300 mA; 2x 4 configurable inputs/outputs, (digital input: 0 to max 40 V DC, digital output: 0 to max 40 V DC, open drain, max 100 mA)</p> <p>Reader data: RS485 full duplex, RS485 half duplex, Wiegand</p> <p>Auxiliary: 1x 3.3 V DC output, max 100 mA, 2x configurable inputs/output (digital input: 0 to max 40 V DC, digital output: 0 to max 40 V DC, open drain, max 100 mA)</p> <p>Door connectors: 2x 2 input for door monitors and REX (digital input: 0 to max 40 V DC)</p>
	I/O functionality	Preconfigured for readers and door monitors, Input trigger, Output toggle/pulse
Network	Security	Password protection, IP address filtering, HTTPS ² encryption, IEEE 802.1X network access control, digest authentication, user access log
	Supported protocols	IPv4, HTTP, HTTPS ² , TLS ² , QoS layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS
System Integration	Application Programming Interface	<p>Open API for software integration, including VAPIX[®]; specifications available at www.axis.com</p> <p>ONVIF Profile C, specifications available at www.onvif.org</p> <p>Support for access control as a service with One-Click Connection</p>
Events & Alarms	Tamper detection	<p>Removal of unit cover/tamper front</p> <p>Removal of unit from wall/tamper back</p> <p>Reader tamper</p>
	Event log	Configurable by time and topic, Alarm acknowledgement
	Event actions	Notification via email, HTTP and TCP, External output port, Status LED
	Event triggers	<p>Access Point: Access point enabled</p> <p>Configuration: Access point changed, Access point removed, Area changed, Area removed, Door changed, Door removed</p> <p>Door: Door alarm, Door double-lock monitor, Door lock monitor, Door mode, Door monitor, Door warning</p> <p>Event Logger: Alarm</p> <p>Hardware: Casing open, Network, peer connection</p> <p>Input Signal Digital input port, Manual trigger, Virtual inputs</p> <p>Schedule: Interval, Pulse</p> <p>System: System ready</p> <p>Time: Recurrence, Use schedule</p>

AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Function/group	Item	Specifications
General	Casing	Plastic
	Software	Configuration and basic access control management through Internet Explorer, Firefox, Chrome, or Safari
	Memory	256 MB RAM, 4 Gbit Flash
	Power	Power in: 10–30 V DC, max 26 W or Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3 Power out & relay: 1x 12 V DC, max 500 mA 1x solid state relay 30 V DC, max 700 mA Power out lock: 2x 12 V DC, max 500 mA ¹
	Connectors	RJ45 10BASE-T/100BASE-TX Terminal blocks: DC power, 10 Inputs/Outputs, RS485/Wiegand, Relay Cable size for connectors: CSA: AWG 28–16, CUL/UL: AWG 30–14
	Operating conditions	0 °C to 50 °C (32 °F to 122 °F) Humidity 20–85% RH (non-condensing)
	Approvals	EN 55022 Class B, EN 50130-4, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 61000-6-1, EN 61000-6-2FCC Part 15 Subpart B Class B ICES-003 Class B C-tick AS/NZS CISPR22 Class B VCCI Class B IEC/EN/UL 60950-1, UL 294, UL 2043, EN 50581
	Dimensions (HxWxD)	45.5 x 180 x 180 mm (1.8 x 7.1 x 7.1 in)
	Weight	500 g (1.1 lb)
	Included accessories	Connector kit, Cable ties, Installation Guide
	Languages	English, German, French, Spanish, Italian
	Warranty	Axis 3-year warranty with possibility to extend up to 5 years, see www.axis.com/warranty
	Optional accessories	AXIS T8120 Midspan 15 W AXIS T8128 PoE Splitter 24 V (requires 30 W midspan) AXIS T8129 PoE Extender Mains adaptor 24 V DC AXIS T98A15-VE Surveillance Cabinet ³

1. Power consumption dependent; max load for readers and other equipment is 7.5 W with PoE and 14 W with 10–30 V DC.
2. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>), and cryptographic software written by Eric Young (eay@cryptsoft.com)
3. In outdoor installations combining AXIS A1001 and AXIS T98A15-VE, the allowed maximum voltage is 30 V DC.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

AXIS Entry Manager

Function/group	Item	Specifications
	Models	AXIS A1001 with built-in web-based software
Door controller	Readers	Up to 2 readers per controller ¹ (Wiegand, RS485 (OSDP) with supported card formats)
	Controllers	1–33
	Credentials	Up to 400
	Event history	30 000 First in First out (FIFO) per system
Digital I/O	I/O interface	Reader I/O: DC output: 2x 12 V DC output max 300 mA; 2x 4 configurable inputs/outputs, (digital input: 0 to max 40 V DC, digital output: 0 to max 40 V DC, open drain, max 100 mA) Reader data: RS485 full duplex, RS485 half duplex, Wiegand Auxiliary: 1x 3.3 V DC output, max 100 mA, 2x configurable inputs/output (digital input: 0 to max 40 V DC, digital output: 0 to max 40 V DC, open drain, max 100 mA) Door connectors: 2x 2 input for door monitors and REX (digital input: 0 to max 40 V DC)
	I/O functionality	Preconfigured for readers and door monitors, Input trigger, Output toggle/pulse
Network	Security	Password protection, IP address filtering, HTTPS ² encryption, IEEE 802.1X network access control, digest authentication, user access log
	Supported protocols	IPv4, HTTP, HTTPS ² , TLS ² , QoS layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS
Events & Alarms	Tamper detection	Removal of unit cover/tamper front Removal of unit from wall/tamper back Reader tamper
	Event log	Configurable by time and topic, Alarm acknowledgement
	Event actions	Notification via email, HTTP and TCP, External output port, Status LED
	Event triggers	Access Point: Access point enabled Configuration: Access point changed, Access point removed, Door changed, Door removed Door: Door alarm, Door double-lock monitor, Door lock monitor, Door mode, Door monitor, Door warning Event Logger: Alarm Hardware: Casing open, Network, peer connection Input Signal Digital input port, Manual trigger, Virtual inputs Schedule: Interval, Pulse System: System ready Time: Recurrence, Use schedule
System features	Access schedules	Unlimited
	Installation & Configuration	Configuration wizard, configuration verification, Color-coded connectors, I/O assignment print-out, Automatic controller discovery, Instant feedback of missing configuration data
	Administration	Drag-and-drop operation with flexible assignment of doors and user groups, Retrieve credentials from reader, Manual access/lock/unlock, Import of users
	Languages	English, German, French, Spanish, Italian

AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Function/group	Item	Specifications
General	Casing	Plastic
	Software	Configuration and basic access control management through Internet Explorer, Firefox, Chrome, or Safari
	Memory	256 MB RAM, 4 Gbit Flash
	Power	Power in: 10–30 V DC, max 26 W or Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3 Power out & relay: 1x 12 V DC, max 500 mA 1x solid state relay 30 V DC, max 700 mA Power out lock: 2x 12 V DC, max 500 mA ¹
	Connectors	RJ45 10BASE-T/100BASE-TX Terminal blocks: DC power, 10 Inputs/Outputs, RS485/Wiegand, Relay Cable size for connectors: CSA: AWG 28–16, CUL/UL: AWG 30–14
	Operating conditions	0 °C to 50 °C (32 °F to 122 °F) Humidity 20–85% RH (non-condensing)
	Approvals	EN 55022 Class B, EN 50130-4, EN 61000-3-2, EN 61000-3-3, EN 55024, EN 61000-6-1, EN 61000-6-2FCC Part 15 Subpart B Class B ICES-003 Class B C-tick AS/NZS CISPR22 Class B VCCI Class B IEC/EN/UL 60950-1, UL 294, UL 2043, EN 50581
	Dimensions (HxWxD)	45.5 x 180 x 180 mm (1.8 x 7.1 x 7.1 in)
	Weight	500 g (1.1 lb)
	Included accessories	Connector kit, Cable ties, Installation Guide
	Warranty	Axis 3-year warranty with possibility to extend up to 5 years, see www.axis.com/warranty
	Optional accessories	AXIS T8120 Midspan 15 W AXIS T8128 PoE Splitter 24 V (requires 30 W midspan) AXIS T8129 PoE Extender Mains adaptor 24 V DC AXIS T98A15-VE Surveillance Cabinet ³

1. Power consumption dependent; max load for readers and other equipment is 7.5 W with PoE and 14 W with 10–30 V DC.
2. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>), and cryptographic software written by Eric Young (eay@cryptsoft.com)
3. In outdoor installations combining AXIS A1001 and AXIS T98A15-VE, the allowed maximum voltage is 30 V DC.

Connectors

For information about the connectors' positions, see *Hardware Overview on page 5*.

For connection diagrams and information about the hardware pin chart generated through the hardware configuration, see *Connection Diagrams on page 61* and *Configure the Hardware on page 13*.

The following section describes the connectors' technical specifications.

AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Reader Data Connector

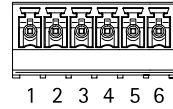
6-pin terminal block supporting RS485 and Wiegand protocols for communication with the reader.

The RS485 ports support:

- Two-wire RS485 half duplex
- Four-wire RS485 full duplex

The Wiegand ports support:

- Two-wire Wiegand



Function		Pin	Notes
RS485	A-	1	For full duplex RS485 For half duplex RS485
	B+	2	
RS485	A-	3	For full duplex RS485 For half duplex RS485
	B+	4	
Wiegand	D0 (Data 0)	5	For Wiegand
	D1 (Data 1)	6	

Important

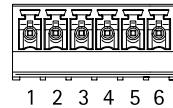
The recommended maximum cable length is 30 m (98.4 ft).

Reader I/O Connector

6-pin terminal block for:

- Auxiliary power (DC output)
- Digital Input
- Digital Output
- 0 V DC (-)

Pin 3 on the reader I/O connectors can be supervised. If the connection is interrupted, an event is activated. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See [page 62](#).



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC output	2	For powering auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 300 mA
Configurable (Input or Output)	3-6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 40 V DC
		Digital output – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protection against voltage transients.	0 to max 40 V DC, open drain, 100 mA

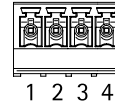
AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Door Connector

Two 4-pin terminal blocks for door monitoring devices (digital input).

All door input pins can be supervised. If the connection is interrupted, an alarm is triggered. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See [page 62](#).



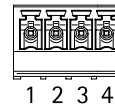
Function	Pin	Notes	Specifications
0 V DC (-)	1, 3		0 V DC
Input	2, 4	For communicating with door monitor. Digital input – Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate. Note: This pin can only be used for input.	0 to max 40 V DC

Auxiliary Connector

4-pin configurable I/O terminal block for:

- Auxiliary power (DC output)
- Digital Input
- Digital Output
- 0 V DC (-)

For an example connection diagram, see [Connection Diagrams on page 61](#).



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC output	2	For powering auxiliary equipment. Note: This pin can only be used as power out.	3.3 V DC Max load = 100 mA
Configurable (Input or Output)	3-4	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 40 V DC
		Digital output – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protection against voltage transients.	0 to max 40 V DC, open drain, 100 mA

Power Connector

2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤ 100 W or a rated output current limited to ≤ 5 A.



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC input	2	For powering controller when not using Power over Ethernet. Note: This pin can only be used as power in.	10–30 V DC, max 26 W Max load on outputs = 14 W

AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Network Connector

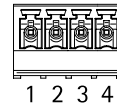
RJ45 Ethernet connector. Supports Power over Ethernet (PoE). Use Category 5e cables or higher.

Function	Specifications
Power and Ethernet	Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3, 44–57 V DC Max load on outputs = 7.5 W

Power Lock Connector

4-pin terminal block for powering one or two locks (DC output). The lock connector can also be used to power external devices.

Connect locks and loads to the pins according to the hardware pin chart generated through the hardware configuration.



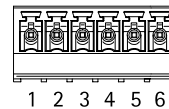
Function	Pin	Notes	Specifications
0 V DC (-)	1, 3		0 V DC
0 V DC, floating, or 12 V DC	2, 4	For controlling up to two 12 V locks. Use the hardware pin chart. See <i>Configure the Hardware on page 13</i> .	12 V DC Max total load = 500 mA

Power & Relay Connector

6-pin terminal block with built-in relay for:

- External devices
- Auxiliary power (DC output)
- 0 V DC (-)

Connect locks and loads to the pins according to the hardware pin chart generated through the hardware configuration.



Function	Pin	Notes	Specifications
0 V DC (-)	1, 4		0 V DC
Relay	2–3	For connecting relay devices. Use the hardware pin chart. See <i>Configure the Hardware on page 13</i> . The two relay pins are galvanically separated from the rest of the circuitry.	Max current = 700 mA Max voltage = +30 V DC
12 V DC	5	For powering auxiliary equipment. Note: This pin can only be used as power out.	Max voltage = +12 V DC Max load = 500 mA
24 V DC	6	Not used	

Tampering Alarm Pin Header

Two 2-pin headers for bypassing:

- Back tampering alarm (TB)
- Front tampering alarm (TF)



AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Function	Pin	Notes
Back tampering alarm	1-2	To bypass the front and back tampering alarm simultaneously, connect jumpers between TB 1, TB 2 and TF 1, TF 2 respectively. Bypassing the tampering alarms means that the system will not identify any tampering attempts.
Front tampering alarm	1-2	

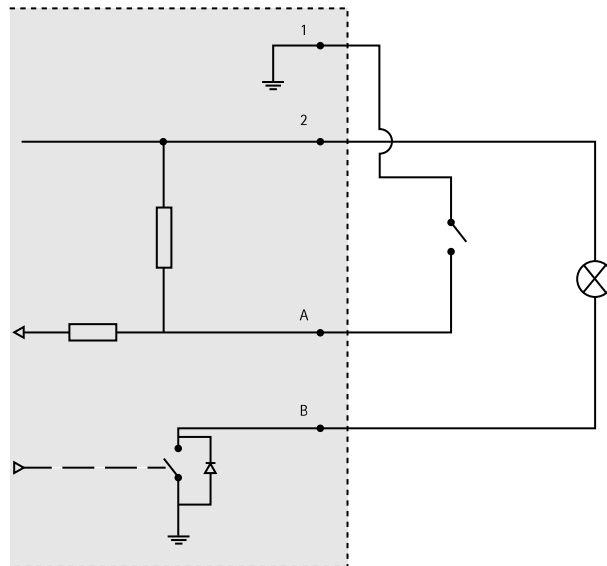
Note

Both the front and back tampering alarms are connected by default. The casing open trigger can be configured to perform an action if the door controller is opened or if the door controller is removed from the wall or ceiling. For information about how to configure alarms and events, see *Alarm and Event Configuration*.

Connection Diagrams

Connect devices according to the hardware pin chart generated through the hardware configuration. For more information about hardware configuration and the hardware pin chart, see *Configure the Hardware on page 13*.

Auxiliary Connector

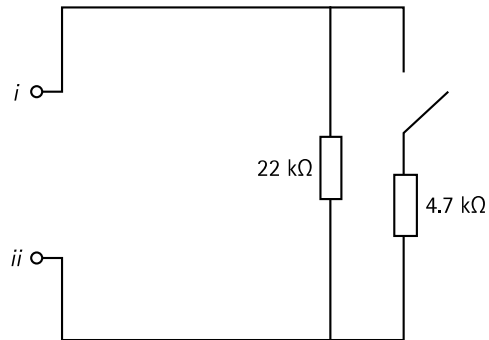


- 1 0 V DC (-)
- 2 DC output: 3.3 V, max 100 mA
- A I/O configured as input
- B I/O configured as output

AXIS A1001 Network Door Controller & AXIS Entry Manager

Technical Specifications

Supervised Inputs



To use supervised inputs, install end of line resistors. This applies to all supervised inputs. For information about limitations and updates, see the product's release notes.

- i* Input
- ii* 0 VDC (-)

